機能詳細編

LAN側の設定 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
セキュリティの設定 ・・・・・・・・・・・・・・・・・・・・・・・・ 45
ポートフォワードの設定 ・・・・・・・・・・・・・・・・・・・・ 99
VPNの設定 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・127
オプション設定 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 159
保守・管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 177

LAN側の設定

ここでは、主に本製品のLAN側の設定について解説します。本製品の設定は、有線LAN接続でおこなってください。

IPアドレスの設定

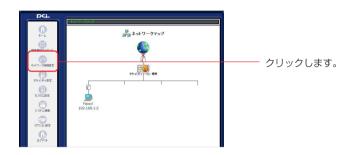
本製品のLAN側ポートのIPアドレスを確認・変更する方法を解説します。

! ご注意

本製品のIPアドレスを変更する場合は、誤ったIPアドレスを設定することのないようご注意ください。誤ったIPアドレスを設定すると、インターネットに接続できなくなるなどのトラブルになることがあります。

LAN側ポートのIPアドレスを確認・変更する

購入時の状態では、本製品のLAN側ポートのIPアドレスは「192.168.1.1」が設定されています。
すでにLANが構築されている環境に本製品を導入した場合などで、本製品のLAN側ポートのIPアドレスを変更する必要があるときは、次の手順で行います。

1 サイドバーから［ネットワーク詳細設定］アイコンをクリックします。

2 ［LAN Ethernet］の、［修正］ボタンをクリックします。

3 ［詳細設定］ボタンをクリックします。

4 本製品のLAN側ポートのIPアドレスは「IP設定」欄に表示されます。IPアドレスを変更するときは、必要に応じて各項目を設定します。

5 画面の一番下にある[OK]ボタンをクリックし、[ネットワーク接続 LAN Ethernet]画面に戻ります。

※[OK]ボタンをクリックして[注意]画面に切り替わる場合には、その内容をご確認の上、さらに[OK]ボタンをクリックして[ネットワーク接続 LAN Ethernet]画面に戻ってください。

6 [OK]ボタンをクリックし、[ネットワーク詳細設定]画面に戻ります。

※WEBブラウザで本製品のIPアドレスを指定して設定ページにアクセスしていた場合、続いて別の設定を行いたいときは、変更後のIPアドレスでアクセスし直してください。

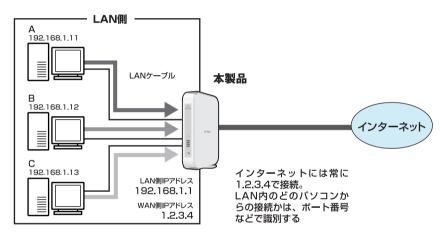
MEMO

●LAN側のIPアドレスを変更したとき
LAN側のIPアドレスやサブネットマスクを変更したときは、変更後の内容に合わせて[DHCPサーバ]の設定も変更してください。

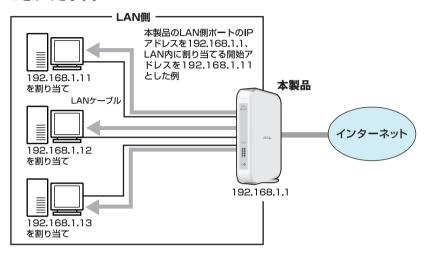
●LAN内で起動しているパソコンがあるとき
本製品のLAN側ポートのIPアドレスを変更するときに、LAN内で起動しているパソコンがある場合は、本製品のIPアドレスを変更した後でIPアドレスを再取得してください。

NAPT（IPマスカレード）

本製品では、ルーティングのモードとしてNAPTに対応しています。

複数のプライベートIPアドレスを1つのグローバルIPアドレスに変換する機能で、IPマスカレードとも呼ばれます。LAN側にプライベートIPアドレスを割り当てたパソコンが複数台あり、1つのグローバルIPアドレスでインターネットに接続する運用形態のときは、NAPTを使用します。
NAPTを使用した場合、LAN内で割り当てられてる複数のプライベートIPアドレスが、インターネットへの接続時に1つのグローバルIPアドレスに変換されます。さらに、ポート番号も変換されます。インターネット側からは、常に1台のパソコンがインターネットに接続しているように見えます。

※NAPT機能を利用するための設定は必要はありません。本製品の運用を開始すると、自動的にNAPT機能は有効になります。

DHCPサーバ設定

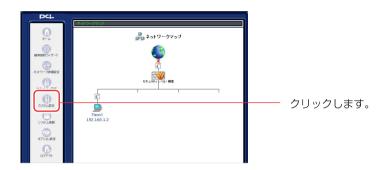
DHCPサーバ機能を利用すると、LAN内のパソコンやネットワーク機器がLANに接続されるたびに、他のどれとも重複しないIPアドレスを自動で割り当てることができます。

本製品のDHCPサーバ機能は、特定のパソコンに常に固定のIPアドレスを割り当てることもできます。
また固定のIPアドレスの割り当てと、動的なIPアドレスの割り当ての両方を設定することもできます。

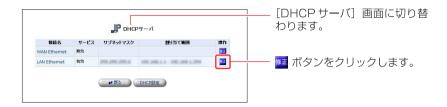
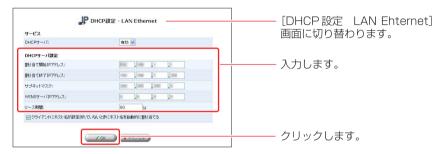
! ご注意

・本製品のDHCPサーバ機能はデフォルトで有効になっています。
・DHCPサーバ機能を使用しないときは、LAN側に接続されているパソコンすべてに、手動でIPアドレスを割り当ててください。
・パソコンに手動でIPアドレスを設定した場合、そのパソコンのホスト名やIPアドレスを本製品で管理することはできません。

DHCP サーバの基本設定

ここでは、DHCP サーバの基本的な設定について説明します

1 サイドバーから[カスタム設定]をクリックします。

2 [DHCP サーバ]をクリックします。

3 現在のDHCPサーバのサブネットマスク、IPアドレスの割り当て範囲が表示されます。設定を変更する場合は、［修正］ボタンをクリックします。

4 [DHCP設定LAN Ethernet]画面が表示されます。
割り当てるIPアドレスの範囲、サブネットマスク、リース期間を設定し、[OK]ボタンをクリックします。

［有効］
DHCPサーバ機能を有効にします。

［割り当て開始IPアドレス］
割り当てるIPアドレスの、開始アドレスを入力します。

［割り当て終了IPアドレス］
割り当てるIPアドレスの、終了アドレスを入力します。

［サブネットマスク］
割り当てるサブネットマスクを入力します。

［WINSサーバ］
WINSサーバを使用してる場合は、サーバアドレスを入力します。

［リース期間（分）］
割り当てるIPアドレスの有効期限を分単位で入力します。

［クライアントにホスト名が設定されていないときにホスト名を自動的に割り当てる］
接続されているパソコンまたはネットワーク機器にホスト名が設定されていない場合、自動的にホスト名が設定されます。

5 [OK]ボタンをクリックし、[DHCP サーバ]画面に戻ります。

6 以上で設定は終了です。

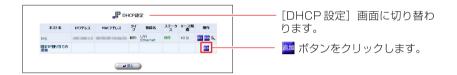
DHCPサーバから固定のIPアドレスを割り当てる

ここでは、特定のパソコンやネットワーク機器にDHCPサーバから常に固定のIPアドレスを割り当てる方法について説明します。

1 サイドバーから[カスタム設定]アイコンをクリックします。

2 [DHCPサーバ]アイコンをクリックします。

3　[DHCP設定]ボタンをクリックします。

4　[固定IP割り当ての追加]欄から[追加]ボタンをクリックします。

5　追加したいパソコンやネットワーク機器のホスト名、IPアドレス、MACアドレスを入力し、[OK]ボタンをクリックします。

[ホスト名]

パソコンまたはネットワーク機器のホスト名を入力します。半角英数字を使用し、1～63文字の範囲で入力してください。

[IPアドレス]

パソコンまたはネットワーク機器に割り当てるIPアドレスを入力します。

[MACアドレス]

IPアドレスを割り当てるパソコンまたはネットワーク機器のMACアドレスを入力します。

6 追加したホストが[DHCP設定]画面に表示されているのを確認します。

7 以上で設定は終了です。

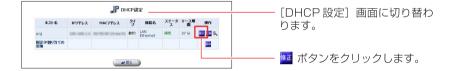
IPアドレスの修正

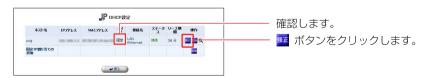
ここでは、既にDHCPサーバから自動にIPアドレスが割り当てられているパソコンまたはネットワーク機器の設定を変更する方法について説明します。

1　サイドバーから[カスタム設定]アイコンをクリックします。

2　[DHCPサーバ]アイコンをクリックします。

3 [DHCP 設定]ボタンをクリックします。

4 設定を変更したいホストの［修正］ボタンをクリックします。

5 [固定割り当て]にチェックを付け、[OK]ボタンをクリックします。

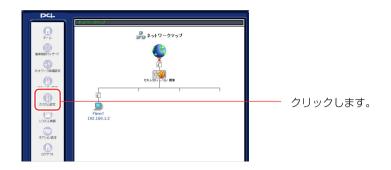
6 タイプが [固定] になっているのを確認し、ホストの[修正]ボタンをクリックします。

7 IPアドレスを固定で割り当てたり、ホスト名、MACアドレスの修正を行うことができます。

8 [OK]ボタンをクリックし、[DHCP設定]画面に戻ります。

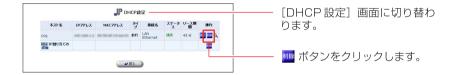
9 以上で設定は終了です。

IPアドレスの削除

ここでは、登録済みのIPアドレスとホスト名の対応を削除する方法について説明します。

1 サイドバーから[カスタム設定]をクリックします。

2 [DHCPサーバ]をクリックします。

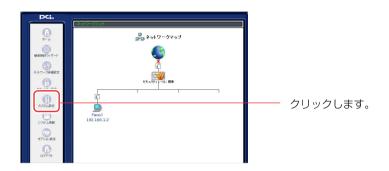
3 [DHCP 設定]ボタンをクリックします。

4 削除したいホストの［削除］ボタンをクリックします。

5 [戻る]ボタンをクリックし、[DHCP サーバ]画面に戻ります。

6 以上で設定は終了です。

DHCP サーバ機能の有効/無効を設定する

ここでは、DHCP サーバ機能の有効/無効を設定する方法について説明します。

1 サイドバーから[カスタム設定]をクリックします。

2 [DHCP サーバ]をクリックします。

3 現在のDHCPサーバのサブネットマスク、IPアドレスの割り当て範囲が表示されます。設定を変更する場合は、［修正］ボタンをクリックします。

4 [DHCPサーバ]欄から[有効]または[無効]を選択します。

! ご注意

・DHCPサーバ機能を無効にした場合は、本製品のLAN側に接続されてるパソコンまたはネットワーク機器に、手動でIPアドレスを設定してください。

5 [OK]ボタンをクリックし、[DHCPサーバ]画面に戻ります。

※［OK］ボタンをクリックして［注意]画面に切り替わる場合には、その内容をご確認の上、さらに［OK］ボタンをクリックして［DHCPサーバ］画面に戻ってください。

6 以上で設定は終了です。

DNSサーバ設定

本製品のDNSサーバは、LAN内のパソコンやネットワーク機器のホスト名とIPアドレスの対応を管理しています。

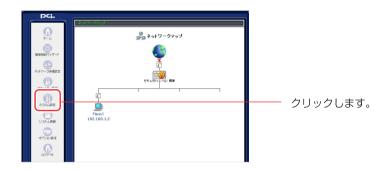
DNSサーバはDHCPサーバと同じ対応表を参照しています。DHCPサーバの設定時にホスト名を登録しておくと、他に特別な設定をせずに、ホスト名および対応するIPアドレスがDNSサーバで管理されます。

! ご注意

・本製品のDNSサーバは、LAN内のドメイン名とIPアドレスの対応だけを管理しています。
・インターネット上のドメイン名を指定した通信では、本製品の「プロキシDNS」機能が使用されます。

DHCPサーバによるホスト名とIPアドレスの確認

本製品のDNSサーバはDHCPサーバと同じ対応表を参照しています。
DHCPサーバでホスト名とIPアドレスを登録した場合は、DNSサーバにも反映されます。
ここでは、DHCPサーバ機能で自動登録されたホスト名とIPアドレスを確認します

1 サイドバーから[カスタム設定]をクリックします。

2 [DHCPサーバ]をクリックします。

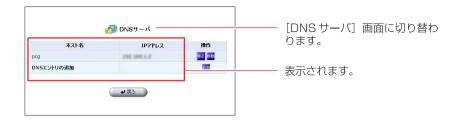
3 [DHCP設定]アイコンをクリックします。

4 DHCPサーバ機能により、本製品に登録されてるホスト名とそのIPアドレスが表示されます。

5 [戻る]ボタンをクリックし、[DHCPサーバ]画面に戻ります。

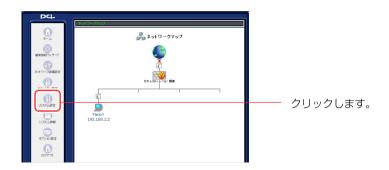
6 [戻る]ボタンをクリックし、[カスタム設定]画面に戻ります。

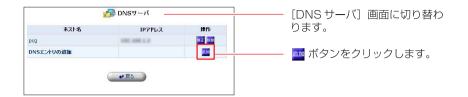
7 [DNSサーバ]アイコンをクリックします。

8　本製品のDNSサーバに登録されてるホスト名とIPアドレスが表示されます。

9　以上で確認は終了です。

ホスト名とIPアドレスを手動で登録する

DHCPサーバ機能を使用しない場合は手動でホスト名とIPアドレスを登録する必要があります。

1　サイドバーから[カスタム設定]アイコンをクリックします。

2　[DNSサーバ]アイコンをクリックします。

3 [DNSエントリの追加]から［追加］ボタンをクリックします。

4 DNSサーバに登録するホスト名とIPアドレスを入力し、[OK]ボタンをクリックします。

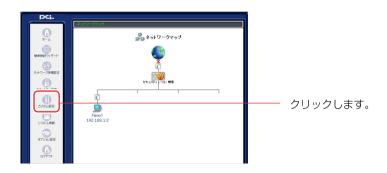
5 以上で設定は終了です。

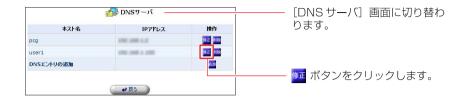
ホスト名とIPアドレスの修正

ホスト名やIPアドレスを変更したときは、DNSサーバに登録した情報も手動で変更する必要があります。

ご注意

・DHCPサーバ機能を有効にしているときは、パソコンのホスト名は自動的にDNSサーバに反映されます。手動でホスト名を変更する必要はありません。

1 サイドバーから[カスタム設定]アイコンをクリックします。

2 [DNSサーバ]アイコンをクリックします。

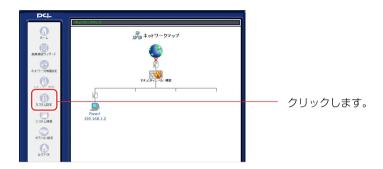
3　情報を修正したいホスト名の［修正］ボタンをクリックします

4　ホスト名とIPアドレスを修正し、[OK]ボタンをクリックします。

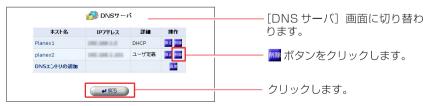
※DHCPサーバによりIPアドレスを割り当てられたホストについては、ホスト名のみ修正が可能です。

5　以上で設定は終了です。

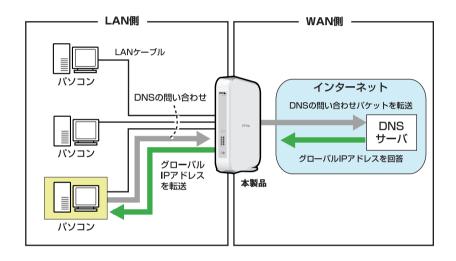
ホスト名とIPアドレスの削除

登録されているホスト名とIPアドレスの削除を行います。

1 サイドバーから[カスタム設定]アイコンをクリックします。

2 [DNSサーバ]アイコンをクリックします。

3 情報を削除したいホスト名の［削除］ボタンをクリックし、［戻る］ボタンをクリックします。

4 以上で設定は終了です。

プロキシDNS

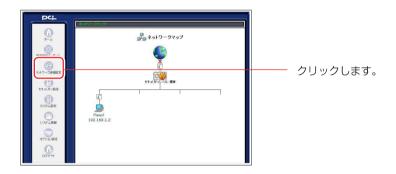
本製品には「プロキシDNS」機能が搭載されています。プロキシDNSとは、LAN側の各パソコンからインターネット上のドメイン名を指定した接続（DNSの問い合わせ）があった場合に、それをインターネット上のDNSサーバにフォワーディングして、対応するIPアドレスを各パソコンに回答する機能です。
LAN側のパソコンからは、インターネット上のDNSサーバに代理で問い合わせていることはわからず、単に、本製品がインターネット上のドメインと各IPアドレスの対応を管理するDNSサーバとして動作しているように見えます。

WAN側で複数セッションを接続している時には、LAN側のパソコンからDNSの問い合わせがあった場合、本製品のプロキシDNS機能は、全てのセッション上のDNSサーバに問い合わせのパケットを送信します。この場合、返答のあったDNSサーバのセッションを使用して通信を行います。2つ以上のセッションのDNSサーバから返答があった場合は、先に返答があった方のセッションを使用します。

ルーティング設定

本製品は、ダイナミックルーティングのプロトコルとしてRIP、RIP Version2に対応しています。また、スタティックルーティングにも対応しています。

ダイナミックルーティングの設定

ここでは、ダイナミックルーティングを設定し、動的に経路情報を登録する方法について説明します。本製品のダイナミックルーティングを設定する場合は、ダイナミックルーティングを有効にするインターフェイスを設定し、本製品のダイナミックルーティング機能を有効にします。

1 サイドバーから［ネットワーク詳細設定］アイコンをクリックします。

2 [接続名]欄からダイナミックルーティングを有効にするインターフェイスの［修正］ボタンをクリックします。

3 ここでは例として［LAN Ethernet]を選択します。他のインターフェイスを選択した場合も同様の手順で進めてください。

4　［ネットワーク接続 LAN Ethernet］画面が表示されます。［詳細設定］ボタンをクリックします。

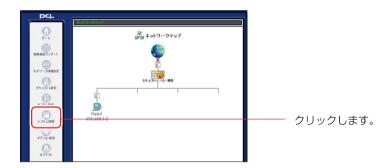
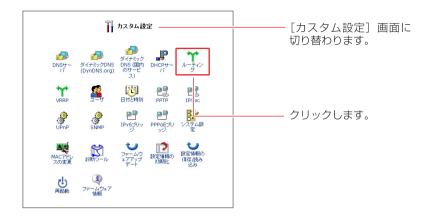
5　［デバイスメトリック］欄から［RIP-ルーティングプロトコル］にチェックをつけます。

6　RIPの送受信設定を行います。［RIP受信設定］欄から本製品が受信するRIPの種類を選択します。［RIP送信設定］欄から本製品から送信するRIPの種類を選択します。

RIP受信設定	
なし	RIP機能を無効にします。
RIPv1	RIPv1による、ルート情報の受信を行います。
RIPv2	RIPv2による、ルート情報の受信を行います。
RIPv1/2	RIPv1/2による、ルート情報の受信を行います。
RIP送信設定	
なし	RIP機能を無効にします。
RIPv1	RIPv1による、ルート情報の送信を行います。
RIPv2・ブロードキャスト	ネットワーク内の不特定多数にRIPv2による、ルート情報の送信を行います。
RIPv2・マルチキャスト	複数の相手を指定してRIPv2による、ルート情報の送信を行います。

7 ［OK］ボタンをクリックします。[注意］画面が表示される場合は、内容を確認したうえで［OK］ボタンをクリックします。

8 ［ネットワーク接続 LAN Ethernet]画面に戻ります。

9 サイドバーから［カスタム設定］アイコンをクリックします。

10［ルーティング］アイコンをクリックします。

11［ルーティングプロトコル］欄から［RIP-ルーティングプロトコル］にチェックがついてるか確認します。

12［OK］ボタンをクリックします。

13 以上で設定は終了です。

スタティックルーティングの経路情報を追加する

ここでは、経路情報を手動で設定する方法について説明します。経路情報の追加は、50以内とすることをお勧めします。※50以上の経路を設定すると、本製品の動作パフォーマンスに影響することがあります。

1 サイドバーから[カスタム設定]アイコンをクリックします。

2 [ルーティング]アイコンをクリックします。

3 [ルートの追加]から[追加]ボタンをクリックします。

4 経路情報を追加するインターフェースを選択し、経路情報を入力して[OK]ボタンをクリックします。

［接続名］

スタティックルーティングを設定する転送先のインタフェースを［LAN Ehternet］、［WAN Ehternet］、［WAN PPPoE］等から選択します。

［送信先］

パケットの送信先となるネットワークアドレスを入力します。

［ネットマスク］

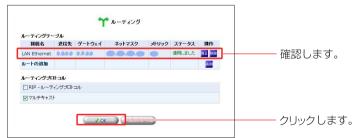
パケットの送信先のネットマスクを入力します。

［ゲートウェイ］

宛先のネットワークに到達するための、最初のゲートウェイのアドレスを入力します。

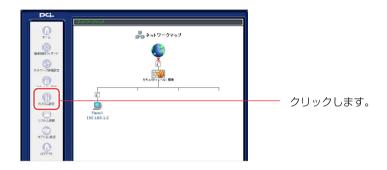
［メトリック］

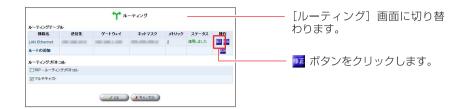
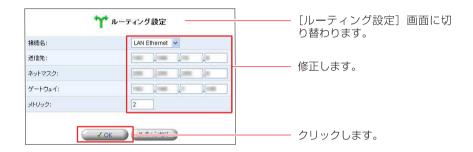
宛先のネットワークに到達するまでのホップカウント（経由するゲートウェイの数）を入力します。

5 [ルーティングテーブル]欄に設定したルーティング情報が追加されていることを確認して[OK]ボタンをクリックします。

6 以上で設定は終了です。

スタティックルーティングの経路情報を修正する

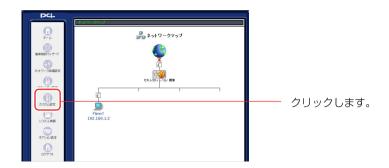
ここでは、既に設定したスタティックルーティングの経路情報を修正する方法について説明します。

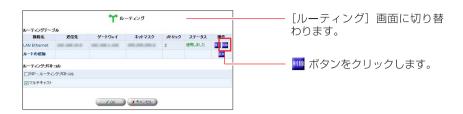
1　サイドバーから[カスタム設定]アイコンをクリックします。

2　[ルーティング]アイコンをクリックします。

3　修正したい経路情報の[修正]ボタンをクリックします。

4　経路情報を修正し、[OK]ボタンをクリックします。

5　以上で設定は終了です。

スタティックルーティングの経路情報を削除する

ここでは、登録したスタティックルーティングを削除する方法について説明します。

1 サイドバーから[カスタム設定]アイコンをクリックします。

2 [ルーティング]アイコンをクリックします。

3 削除したい経路情報の[削除]ボタンをクリックします。

4 [OK]ボタンをクリックします。

5 以上で設定は終了です。

UPnP設定

Universal Plug and Play（UPnP：ユニバーサルプラグアンドプレイ）は、ネットワークに接続するだけで、ネットワーク上の機器同士で簡単に通信できるようにする規格です。本製品は、UPnPに対応しており、次の機能を使用できます。

※購入時の設定でUPnPがONになっているため、特別な設定をする必要がありません。

- UPnPに対応しているOS（Windows® XPとWindows® Me）から、本製品を検出できます。
- UPnPに対応しているOS（Windows® XPとWindows® Me）から本製品の状態を確認したり、設定を一部変更できます。
- 本製品に接続されているLAN内のパソコンから、Windows® MessengerやMSN® Messengerなど、UPnPに対応しているアプリケーションを使用することができます。

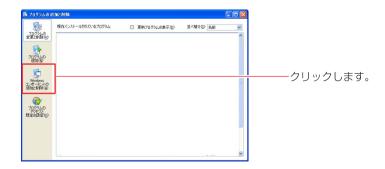
なお、Windows® 98、Windows® 2000およびMacintosh® はUPnPに対応していません。したがって、UPnPの機能を使用することはできません。

パソコンのUPnPの設定を確認する

お使いのパソコンが、UPnPが使用できる状態になっているか確認してください。

■ Windows® XPの場合

1 ［スタート］ボタンをクリックし、［コントロールパネル］をクリックします。

2 ［プログラムの追加と削除］ボタンをクリックし、画面左側にある［Windowsコンポーネントの追加と削除］ボタンをクリックします。

3 [コンポーネント] 欄から [ネットワークサービス] を選択し、[詳細] ボタンをクリックします。

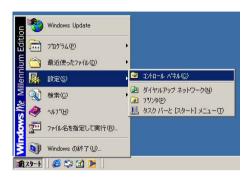
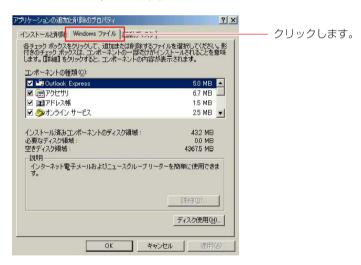
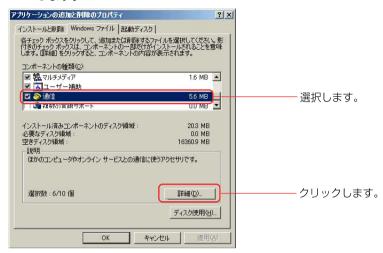
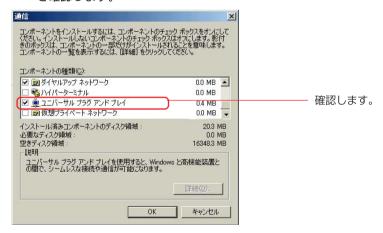
4 ネットワークサービスの詳細が表示されますので、[UPnP ユーザーインターフェイス] の状態を確認します。

[UPnP ユーザーインターフェイス] がチェックされているときは、パソコンの UPnP の機能が有効になっています。ダイアログを閉じてください。

チェックされていないときは、[UPnP ユーザーインターフェイス] が無効になっています。チェックを付け、[OK] ボタンをクリックします。画面の指示に従って、インストールを続けてください。

5 以上で設定は終了です。

■ Windows® Meの場合

1 ［スタート］ボタンをクリックし、［設定］→［コントロールパネル］の順にクリックします。

2 ［アプリケーションの追加と削除］ボタンをクリックします。［アプリケーションの追加と削除］ダイアログが表示されたら、［Windows ファイル］タブをクリックします。

3 [コンポーネントの種類] 欄から [通信] を選択し、[詳細] ボタンをクリックします。

4 通信の詳細が表示されますので、[ユニバーサルプラグアンドプレイ] の状態を確認します。

5 [ユニバーサルプラグアンドプレイ] がチェックされているときは、パソコンがUPnPの機能が有効になっています。ダイアログを閉じてください。

チェックされていないときは、[ユニバーサルプラグアンドプレイ] が無効になっています。チェックを付け、[OK] ボタンをクリックします。画面の指示に従ってインストールを続けてください。

6 以上で設定は終了です。

本製品のUPnP機能をOFFにする

本製品でUPnP機能を使用しないときは、次のように操作します。

1 サイドバーの［カスタム設定］アイコンをクリックします。

2 ［UPnP］アイコンをクリックします。

3 UPnPの機能をOFFにするときは、チェックボックスのチェックを外します。

4 ［OK］ボタンをクリックします。

5 以上で設定は終了です。

セキュリティの設定

本製品の設定は、有線LAN接続でおこなってください。

セキュリティ機能

インターネットに接続すると、LAN内のパソコンがインターネットからの攻撃を受けたり、不正なアクセスをされるという危険があります。そのため、LANを保護する十分なセキュリティ対策を行うことが、快適にインターネットを使う上で重要なポイントとなります。
本製品では、インターネットへの常時接続を行う上でのセキュリティ対策として次の機能を搭載しています。

NAPT（IPマスカレード）	プロバイダから取得したグローバルIPアドレスを、LAN内のプライベートIPアドレスに変換する機能により、インターネット側からLAN内のパソコンを特定できず、アクセスすることができません。このため、外部からの不正アクセスが困難になります。
ステートフル・パケット・インスペクション	ファイアウォール方式として、ステートフル・パケット・インスペクション方式を採用しています。通信セッションごとにパケットの整合性を確認し、必要なポートだけを開くようにします。通信が終了すると利用したポートを遮断します。 さらに、インターネット側からのDoS（Denial of Services）攻撃パターンを識別し、不正なアクセスを遮断することが可能です。
ALG（Application Level Gateway）	アプリケーションレベルでパケットの通過・遮断を判断します。
パケットフィルタリング	インターネットから送られてきたパケットを検査して通過させるかどうかを判断する機能です。どのような条件でパケットを通過させるか、遮断するかをプロトコル/ポートごとに任意に設定できます。
バーチャルコンピュータ	LAN内の1台のパソコンをバーチャルコンピュータホストとすると、WAN側からの全ての接続要求がバーチャルコンピュータホストに転送されるようになります。
ID・パスワードによるユーザ認証	本製品の設定を変更するには、ログインIDとパスワードが必要です。

セキュリティレベル設定

ここでは、本製品の基本的なセキュリティレベルの設定を行います。
セキュリティ対策を考える時は、実際のデータのやり取りの流れに合わせて「LANからインターネットへの通信」と「インターネットからLANへの通信」のそれぞれに対してルールを考える必要があります。
一般的には、LANからインターネットにはアクセスできるようにし、インターネットからLANにはアクセスを拒否するように設定します。

本製品のセキュリティ機能には3段階のレベルがあらかじめ用意されています。さらに、用途に応じて設定をカスタマイズすることができます。

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 必要に応じて、レベルを変更します。

セキュリティレベル	**インターネット側からの接続要求**	**LAN内のパソコンからの接続要求**
最大	**拒否** インターネット側からLANにアクセスできません。ただし、［ローカルサーバ］と［リモートアクセス］画面で設定したサービスは使用できます。	**制限あり** LAN内のパソコンで、WEBサービス、e-mailなどのよく使うインターネットのサービスのみ使用できます。※
標準	**拒否** インターネット側からLANにアクセスできません。ただし、［ローカルサーバ］と［リモートアクセス］画面で設定したサービスは使用できます。	**制限なし** LAN内のパソコンで、すべてのインターネットのサービスが使用できます。
最小	**制限なし** インターネットからLANへのアクセスをすべて許可します。	**制限なし** LAN内のパソコンで、すべてのインターネットのサービスが使用できます。

※［セキュリティレベル最大］を選択しているとき、LAN側のパソコンから使用できるインターネットのサービスは次のとおりです。
Telnet、FTP、HTTP、HTTPS、DNS、IMAP、POP3、SMTP

ご注意

［セキュリティレベル最小］を選択すると、セキュリティ機能が一切適用されなくなりますので、必要な場合にのみ設定してください。

3　［IP フラグメントパケットを遮断する］をチェックします。

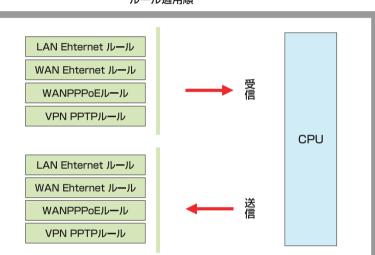
フラグメント化されたデータパケットを利用した攻撃を防ぐことができます。

※IPSec を利用する仮想プライベートネットワークや UDP をベースにしたサービスによっては、IP フラグメントを利用するものがあります。このようなサービスを利用するときは、チェックを外してください。

4　［OK］ボタンをチェックします。

選択したセキュリティレベルに変更されます。

パケットフィルタリング設定

本製品のパケットフィルタの機能は、本製品が受信したパケット、送信するパケットに対してあらかじめ設定してあるフィルタルールを適用します。
フィルタルールには、[LAN Ehternet ルール]、[WAN Ehternet ルール]、[WAN PPPoEルール]等があります。

パケットフィルタの設定

ここでは、本製品にパケットフィルタを設定する方法について説明します。

■パケットフィルタの新規設定

1 サイドバーから[セキュリティ設定]アイコンをクリックします。

2 [パケットフィルタ]タブをクリックします。

3 [セキュリティ設定]画面が表示されます。

4 [受信パケット]欄、または[送信パケット]欄からルールを作成するインターフェースをクリックします。

※ここでは、例として[WAN PPPoEルール]を選択します。他のインターフェースを選択した場合は同様の手順で設定してください。

本製品で設定できるルール一覧

[LAN Ehternet ルール] LANのポートに対して適用されるルールになります。
[WAN Ehternet ルール] WANのポートに対して適用されるルールになります。
[WAN PPPoEルール] WAN PPPoEのポートに対して適用されるルールになります。
[VPN PPTPルール] VPN PPTPの接続に対して適用されるルールになります。

5 [WAN PPPoEルール設定]画面が表示されます。
[新規作成]欄から［追加］ボタンをクリックします。

[WAN PPPoE ルール設定] 画面に切り替わります。

追加 ボタンをクリックします。

6 [フィルタルールの追加]画面が表示されます。

[フィルタルールの追加] 画面に切り替わります。

7 [IPアドレス]欄から送信元IPアドレス、送信先IPアドレスを入力します。

[すべて]を選択した場合は、全てのIPアドレスが対象になります。

選択します。

[1個を指定]を選択した場合は、指定したIPアドレスが対象になります。

入力します。

[範囲指定]を選択した場合は、指定したIPアドレスの範囲が対象になります。

入力します。

8 [動作]欄からフィルタの動作を選択します。

選択します。

[破棄する]
　パケットを破棄します。

[拒否する]
　パケットを破棄して、TCP Reset または ICMP Host Unreachable パケットを送信元に送信します。

[転送する]
　このルールに合致するパケットと、このパケットに関わるセッションのパケットを転送します。

[転送する(パケット)]
　このルールに合致するパケットのみを転送します。

9 [サービス名]欄に本製品に既に登録されているサービスやアプリケーションが表示されます。フィルタルールの対象となるサービスにチェックをつけます。

※リストにないサービスをフィルタする場合は、「新規にサービスを作成する場合」を参照してください。

10 [OK]ボタンをクリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

11 複数のフィルタルールを作成する場合は、3～10の手順を繰り返します。

12 以上で設定は終了です。

■パケットフィルタの修正

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[パケットフィルタ]タブをクリックします。

3　設定を変更したいインターフェースの［修正］ボタンをクリックします。

［セキュリティ設定］画面に切り替わります。

4　[WAN PPPoEルール設定]の画面が表示されますので、[操作]欄から［修正］ボタンをクリックします。

［WAN PPPoEルール設定］画面に切り替わります。

修正ボタンをクリックします。

5 [フィルタルールの編集]画面が表示されますので、必要な項目の修正を行い[OK]ボタンをクリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

6 以上で修正は終了です。

■パケットフィルタの削除

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[パケットフィルタ]タブをクリックします。

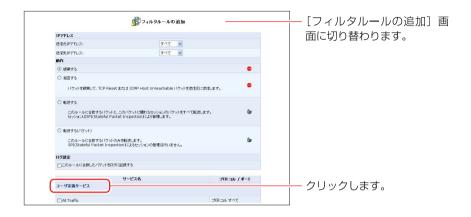
3 設定を削除したいインタフェースの[修正]ボタンをクリックします。

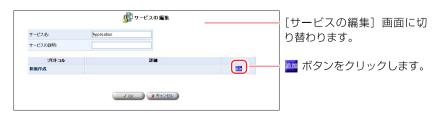
4 [WAN PPPoEルール設定]画面が表示されます。[操作]欄から［削除］ボタンをクリックします。

5 以上で削除は終了です。

新規にサービスを作成する場合

ここでは、本製品にあらかじめ登録されていないサービスを設定する方法について説明します。

1 [フィルタルールの追加]画面から、[ユーザ定義サービス]をクリックします。

2 [ユーザ定義サービス]画面が表示されます。[新規作成]欄から［追加］ボタンをクリックします。

3 [サービスの編集]画面が表示されます。[新規作成]欄から［追加］ボタンをクリックします。

4 [プロトコル]欄から使用するプロトコルを選択します。

[プロトコル]

対象にするプロトコルをTCP、UDP、ICMP、GRE、ESP、AH、その他から選択します。

[送信元ポート/送信先ポート]

サービスやアプリケーションの発信元ポート/送信先ポート番号を入力します。

すべて　→全てのポートを指定します。
１個を指定　→１つのポート番号を指定します。
範囲指定　→ポート番号の範囲を指定します。

[ICMP メッセージ]

対象にするICMP メッセージを選択します。

5 [OK]ボタンをクリックします。

6 ［追加］ボタンをクリックすることで、複数のポートを指定することもできます。

7 全ての設定が終了しましたら［サービス名］に任意の名前を入力し、[OK]ボタンをクリックします。

8 [ユーザ定義サービス] の画面に戻ります。[サービス名] 欄に作成したユーザ定義サービスが表示されるのを確認します。
[戻る] ボタンをクリックします。

9 新規に作成したサービスが[ユーザ定義サービス]欄に表示されます。

10 以上で設定は終了です。

フィルタルールの例

ここでは、パケットフィルタの例としてNetBIOS関連で使われてるポート137～139のLANからWANへの通信を遮断する方法について説明します。
Windows®のLANで使われているNetBIOSのパケットにより、予期せぬインターネットへの通信が発生する場合があります。NetBIOS関連で使われてるポート137～139を遮断することで、予期せぬ通信を防ぎます。

方向	動作	プロトコル	送信元IPアドレス	送信先IPアドレス	送信元ポート	送信元IPアドレス
送信→WAN Ehternet	破棄	TCP/UDP	すべて	すべて	すべて	137～139,445

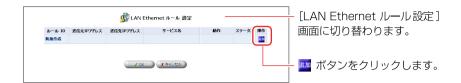
※WindowsMe/98SEの場合、「445」を設定する必要はありません。

1 サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[パケットフィルタ]タブをクリックします。

3　LAN側からWAN側へのNetBIOSのパケットを遮断するルールを作成します。

[受信パケット]欄から[LAN Ehternet ルール]の［修正］ボタンをクリックします。

4 [新規作成]欄から［追加］ボタンをクリックします。

5 送信元IPアドレスに[すべて]、送信先IPアドレスに[すべて]を選択します。

6 [動作]欄から[破棄する]にチェックを付けます。

7 [ユーザ定義サービス]をクリックします。

8 [ユーザ定義サービス]画面が表示されます。[新規作成]欄から［追加]ボタンをクリックします。

9 [サービスの編集]の画面が表示されます。[新規作成]欄から［追加］ボタンをクリックします。

10 プロトコルから[TCP]を選択します。送信元ポートに[すべて]、送信先ポートに[範囲指定]を選択し、ポート番号に「137」～「139」を入力します。

※Windows XP/2000のときは、同じ手順で「445」も設定します。

11 [OK]ボタンをクリックします。

12 同様にUDPポートも遮断しますので、［追加］ボタンをクリックします。

13 プロトコルから[UDP]を選択します。送信元ポートに[すべて]、送信先ポートに[範囲指定]を選択し、ポート番号に「137」～「139」を入力します。

14 [OK]ボタンをクリックします。

15 ［サービスの編集］画面が表示されますので、サービス名に登録する名前を入力し、［OK］ボタンをクリックします。

16 ［ユーザ定義サービス］画面に戻ります。［サービス名］欄に作成したユーザ定義サービスが表示されるのを確認します。［戻る］ボタンをクリックします。

17 [ユーザ定義サービス]欄に作成したサービスが表示されますので、チェックを付け[OK]ボタンをクリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

18 [OK]ボタンをクリックし、[パケットフィルタ]の画面に戻ります。

19 [OK]ボタンをクリックします。

20 次に送信パケットの設定を行います。
[送信パケット]欄から[WAN PPPoEルール]の［修正］ボタンをクリックします。

21 [新規作成]欄から［追加］ボタンをクリックします。

［WAN PPPoE ルール設定］画面に切り替わります。

追加 ボタンをクリックします。

22 送信元IPアドレスに[すべて]、送信先IPアドレスに[すべて]を選択します。

［フィルタルールの追加］画面に切り替わります。

選択します。

23 [動作]欄から[破棄する]にチェックを付けます。

チェックします。

24 [ユーザ定義サービス]欄に先ほど作成したサービスが表示されますので、チェックを付け、[OK]ボタンをクリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

25 [OK]ボタンをクリックし、[パケットフィルタ]の画面に戻ります。

26 以上で設定は終了です。

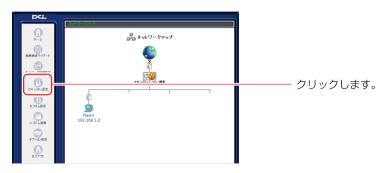
リモートアクセス設定

リモートアクセス機能を使うことで、インターネット側から本製品にアクセスし、各種設定を行うことができます。
デフォルト設定では,LANを保護するためにリモートアクセスを許可していません。

ご注意

不正アクセスにより本製品の設定を変更されないよう、通常はリモートアクセスを無効に設定しておき、必要な場合のみ許可するようにしてください。
本製品に設定されたリモートアクセス機能は、ローカルサーバ、バーチャルコンピュータより優先されます。

リモートアクセスの設定

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［リモートアクセス設定］タブをクリックします。

3　WAN側からのアクセスに関する設定を行います。

設定画面	WEBサーバを外部に公開する（プライマリポート）	本製品のHTTPポートをTCP80ポートで外部に公開する場合に選択します。
	WEBサーバを外部に公開する（セカンダリポート）	本製品のHTTPポートをTCP8080ポートで外部に公開する場合に選択します。
	設定画面を外部に公開する	本製品の設定画面を外部に公開する場合に選択します。上記「プライマリポート」、または「セカンダリポート」をあわせてチェックします。
診断ツール	Pingに応答する	Pingコマンドに返答する場合は選択します。
	UDPTracerouteを許可する	Tracerouteコマンドなどで、UDP上のルート確認をする場合は選択します。
オプション設定		USBカメラから画面を外部に公開する場合に選択します。

ご注意

- Windows® からTracerouteコマンドを使用して、ルートの追跡を行う場合は［Pingに応答する］をチェックしてください。
- 設定画面をWAN側から見るには、以下のURLを指定してアクセスします。
  設定画面用アドレス：http://（WAN側アドレス）/setting/

4　［OK］ボタンをクリックします。

5　以上で設定は終了です。

サイトフィルタ設定

サイトフィルタ機能を使うことで、LAN側のパソコンから特定のWEBサイトを閲覧できないように設定できます。

例えば、公序良俗に反するようなWEBサイトをあらかじめ本製品に設定しておくことで、LAN側のパソコンからそのサイトの閲覧を禁止することができます。
サイトフィルタの登録件数は、50以内とすることをお勧めします。
※50以上の登録すると、本製品の動作パフォーマンスに影響することがあります。

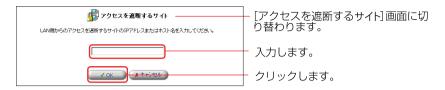
サイトフィルタの設定

■サイトフィルタの新規作成

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［サイトフィルタ］タブをクリックします。

3 ［新規作成］欄から［追加］ボタンをクリックします。

4 閲覧を禁止したいWEBサイトのURLまたはIPアドレスを入力し、[OK]ボタンをクリックします。

5 [IPアドレスまたはホスト名]の一覧に設定したWEBサイトが追加されます。

6 URLが追加されると、追加されたURLがインターネット上に存在するか自動的にチェックします。この間、[ステータス]欄には[確認中]と表示されます。[表示の更新]ボタンをクリックして、入力されたURLが適切なものか確認します。

7 ［OK］ボタンをクリックすると、設定が有効になります。

8 以上で設定は終了です。

MEMO

ステータスに［Error］が表示される場合

→WEBブラウザを起動し設定したURLを入力し、WEBブラウザに表示されるか確認してください。正しく表示されたときは、本製品に設定したURLが間違ってる可能性があります。

■サイトフィルタの有効/無効の切替

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［サイトフィルタ］タブをクリックします。

3 ［IPアドレスまたはホスト名］欄からサイトフィルタを無効にしたいWEBサイトのチェックを外し、［OK］ボタンをクリックします。

4 ［ネットワークマップ］画面がを表示されます。再度［セキュリティ設定］アイコンをクリックし、[サイトフィルタ]タブをクリックします。

5 ［サイトフィルタ］を表示します。［ステータス］表示が［無効］に替わります。再度、サイトフィルタを有効にする場合はチェックを付けます。

6 以上で設定は終了です。

■サイトフィルタの修正

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［サイトフィルタ］タブをクリックします。

3 設定を変更したいWEBサイトのIPアドレスの［修正］ボタンをクリックします。

4 ［アクセスを遮断するサイト］の画面が表示されましたら、新しいIPアドレス、またはホスト名を入力し、［OK］ボタンをクリックします。

5 ［IPアドレスまたはホスト名］の一覧に変更したWEBサイトが表示されます。

6 以上で設定は終了です。

■サイトフィルタの削除

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［サイトフィルタ］タブをクリックします。

3 設定を削除したいWEBサイトのURLの［削除］ボタンをクリックします。

4 ［OK］ボタンをクリックします。

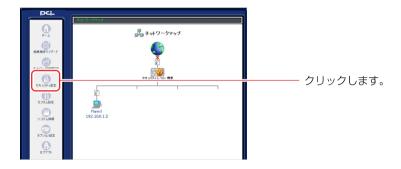
5 以上で設定は終了です。

ログの管理

ここでは、LAN 側のパソコンからインターネットへの接続やインターネット側からLAN への接続、設定ページへのアクセスなどのログ情報を設定します。

セキュリティログの確認

■ログを見る

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［セキュリティログ］タブをクリックします。

3 ［セキュリティログ］画面が表示されます。現在のセキュリティに関するログが確認できます。

■ログの見方（例）

イベント	種類	説明
Inbound/ Outbound Traffic	Connection accepted	接続要求がファイアウォールのセキュリティポリシーに適合していた場合に表示されます。
	Accepted - Host probed	ファイアウォールのセキュリティポリシーに適合したTCP接続要求があったが、インターネット側のホストが信頼できるかどうかわからない場合に表示されます。この場合、インターネット側のホストに認証が試みられます。 ※インターネット側からの接続要求に対してのみ表示されます。
	Accepted - Host trusted	認証を試みていたホストから応答があった場合に表示されます。 ※インターネット側からの接続要求に対してのみ表示されます。
	Accepted - Internal traffic	すべてのパケットがLAN側のホスト同士の間で自由に行き来できる場合に表示されます。
	Connection Refused- Policy violation	接続要求がファイアウォールのセキュリティポリシーに違反している場合に表示されます。
	Blocked - IP Fragment	ファイアウォールですべてのIPフラグメントをブロックする設定を行った場合で、IPフラグメントがブロックされたときに表示されます。エラーはブロックされたフラグメントごとに表示されます。
	Blocked - IP Source Routes	IPヘッダに始点経路制御オプションが設定されていることが原因で、パケットがブロックされたときに表示されます。
	Blocked - State-table error	ファイアウォールによってステートテーブル（LAN側のパソコンやネットワーク機器間のセッション状態に関する情報）が調査または操作されている間に、エラーがあった場合に表示されます。パケットはブロックされます。
Firewall Setup	Aborting configuration	ファイアウォールに関する設定がキャンセルされたときに表示されます。
	Configuration completed	ファイアウォールに関する設定が完了したときに表示されます。

WBM Login	Authentication Success	設定ページへのログインが成功したときに表示されます。
	Authentication Failure	設定ページへのログインが失敗したときに表示されます。
System Up/Down	The system is going DOWN for reboot	本製品を再起動するために終了したときに表示されます。
	The system is UP!	本製品が起動したときに表示されます。

■ログのクリア

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［セキュリティログ］タブをクリックします。

3 ［ログのクリア］ボタンをクリックすると、画面に表示されているログが消去されます。

4 ［戻る］ボタンをクリックします。

5 以上で設定は終了します。

■ログの詳細設定

ここでは、ログの保存に関する設定について説明します。

1　サイドバーから［セキュリティ設定］アイコンをクリックします。

2　［セキュリティログ］タブをクリックします。

3 ［詳細設定］ボタンをクリックします。

4 ［ログイベント］欄から保存するログ内容を選択します。

［許可した接続］

ファイアウォールの通過を許可されたものがログに保存されます。

［拒否した接続］

ファイアウォールの通過を拒否されたものがログに保存されます。

［接続状態］

接続の有効・無効の切替えをログに保存します。

［IPアドレスを詐称した接続］

送信元IPアドレスを詐称してファイアウォールの通過を拒否されたものがログに保存されます。

ご注意

全てのチェックをオンにすると、本製品のパフォーマンスが低下する可能性があります。

5 ［ログバッファ］欄からログ容量が一杯になったときの設定を選択します。

［ログ容量が一杯になったらログを停止する］

ログを保存するメモリが一杯になったときにログの保存を停止する場合は、チェックします。
ログを保存するメモリが一杯になったとき古いログを消去し、続けてログを保存する時はチェックを外します。

6 ［OK］ボタンをクリックします。

7 以上で設定は終了します。

E-Mail通知機能の設定

本製品は、システムや回線、ファイアウォールに何かしらの異常が発生した場合電子メールで管理者に通知することができます。

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［ユーザ］アイコンをクリックします。

3　E-mail通知機能を設定するユーザの［修正］ボタンをクリックします。

4　［E-mailアドレス］欄に、送信先のMailアドレスを入力します。

5 ［システム通知レベル］欄から通知する内容を選択します。
システム通知は、システム情報に関するメッセージを送信します。

［エラー］
本製品が正しく動作していないなどの、致命的なエラーが発生した際にメッセージを送信します。

［警告］
注意を要するエラーが発生した際にメッセージを送信します。
警告を選択した場合は、エラーレベルのメッセージも送信されます。

［情報］
ユーザが本製品を利用したときに表示されるメッセージが送信されます。
情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

6 ［セキュリティ通知レベル］欄から通知する内容を選択します。
セキュリティ通知は、セキュリティログに表示されるメッセージを送信します。

［エラー］

重大なセキュリティイベントが発生した際に、メッセージを送信します。

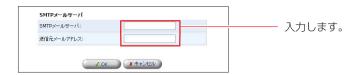
［警告］

注意を要するセキュリティイベントが発生した際にメッセージを送信します。
警告を選択した場合は、エラーレベルのメッセージも送信されます。

［情報］

ユーザが本製品を利用したときに表示されるメッセージが送信されます。
情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

7 本製品からメールを送信するための、SMTP メールサーバの設定をします。
［SMTP メールサーバの設定］をクリックします。

8 ［SMTP メールサーバ］欄にメールサーバのアドレスを入力します。
［送信元メールアドレス］欄に送信元のメールアドレスを入力します。

9 ［OK］ボタンをクリックし、［ユーザ設定］画面に戻ります。

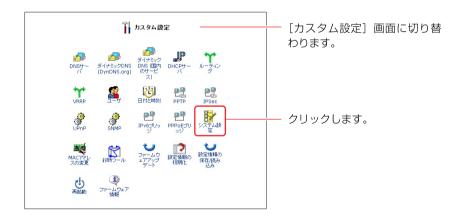
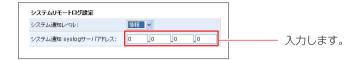
10 ［OK］ボタンをクリックします。

11 以上で設定は終了です。

Syslogの設定

本製品には、システムや回線、ファイアウォールに何かしらの異常が発生した場合Syslogサーバにログを送信することができます。
ここでは、ログをSyslogサーバに送信するための設定を説明します。

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［システム設定］アイコンをクリックします。

3 ［システム通知レベル］欄から通知する内容を選択し、［システム通知Syslogサーバアドレス］にsyslogサーバのアドレスを入力します。

［エラー］

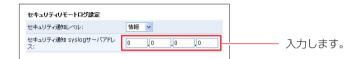
システムに関する重大なメッセージを送信します。

［警告］

システムに関する注意を要するメッセージを送信します。
警告を選択した場合は、エラーレベルのメッセージも送信されます。

［情報］

ユーザが本製品を利用したときに表示されるメッセージが送信されます。
情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

4 ［セキュリティ通知レベル］欄から通知する内容を選択し、［セキュリティ通知 syslog サーバアドレス］にSyslogサーバのアドレスを入力します。
セキュリティ通知は、セキュリティログに表示されるメッセージを送信します。

［エラー］
重大なセキュリティイベントに関するメッセージを送信します。

［警告］
注意を要するセキュリティイベントに関するメッセージを送信します。
警告を選択した場合は、エラーレベルのメッセージも送信されます。

［情報］
ユーザが本製品を利用したときに表示されるメッセージが送信されます。
情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

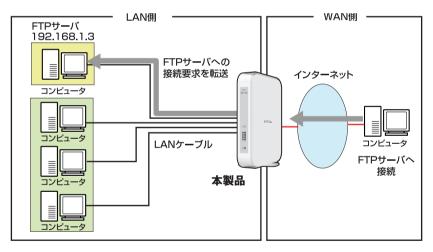
5 ［OK］ボタンをクリックします。

6 以上で設定は終了です。

ポートフォワードの設定

ここでは、LAN 側に設定したパソコンを公開するときに必要な設定について説明します。
本製品の設定は有線LAN 接続でおこなってください。

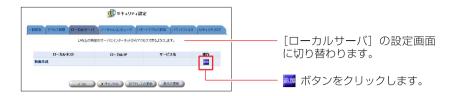
ローカルサーバ設定

LAN 側のサーバをインターネットに公開するときや、オンラインゲームやチャットなどのソフトウェアを使うときはローカルサーバ機能の設定を行います。
本製品には、あらかじめインターネットで使われるサービスやアプリケーションが登録されており、簡単に設定することができます。

ローカルサーバの設定

ここでは、ローカルサーバの詳細な設定を行います。

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[ローカルサーバ]タブをクリックします。

3 [新規作成]欄から［追加］ボタンをクリックします。

4 [ローカルサーバの追加]画面が表示されます。

[ローカルホスト]欄にローカルサーバを設定するパソコンのIPアドレスを入力します。

5 [デフォルト定義サービス]欄に本製品に既に登録されているサービスやアプリケーションが表示されます。インターネットに公開するサービスや、使用するアプリケーションを選択し、チェックします。

※リストにないサービスを使用する場合は、「新規に作成したサービスでローカルサーバを設定する場合」を参照してください。

6 [OK]ボタンをクリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

7 以上で設定は終了です。

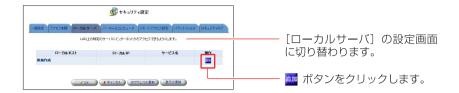
新規に作成したサービスでローカルサーバを設定する場合

■ユーザ定義サービスの新規作成

ここでは、本製品にあらかじめ登録されていないサービスを設定し、ローカルサーバを利用する方法について説明します。

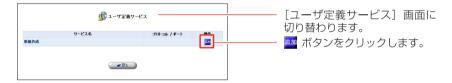
1 サイドバーから[セキュリティ設定]アイコンをクリックします。

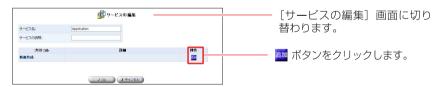
2 [ローカルサーバ]タブをクリックします。

3 [新規作成]欄から［追加］ボタンをクリックします。

4 新規サービスを登録します。

[ユーザ定義サービス]をクリックします。

5 [ユーザ定義サービス]画面が表示されます。

[新規作成]欄から[追加]ボタンをクリックします。

6 [サービスの編集]画面が表示されます。

[新規作成]欄から[追加]ボタンをクリックします。

6 [プロトコル]欄から使用するプロトコルを選択し、ポート番号を入力します。

[プロトコル]

対象にするプロトコルをTCP、UDP、ICMP、GRE、ESP、AH、その他から選択します。その他を選択したときは、対象にするプロトコル番号を直接指定してください。

[送信元ポート/送信先ポート]

サービスやアプリケーションのポート番号を入力します。
すべて　→全てのポートを指定します。
1個を指定→1つのポート番号を指定します。
範囲指定　→ポート番号の範囲を指定します。

[ICMPメッセージ]

対象にするICMPメッセージを選択します。

7 [OK]ボタンをクリックします。

8 さらに［追加］ボタンをクリックすることで、複数のポートを指定することもできます。

9 全ての設定が終了しましたら、[サービス名]欄に任意の名前を入力し、[OK]ボタンをクリックします。

10 [ユーザ定義サービス]の画面に戻ります。

[サービス名]欄に作成したユーザ定義サービスが表示されてるのを確認します。[戻る]ボタンをクリックします。

11 [ローカルサーバの追加]の画面に戻ります。

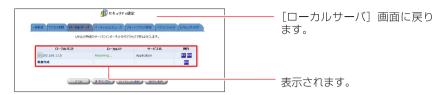
[ユーザ定義サービス]欄に作成したユーザ定義サービスが表示されてるのを確認し、チェックします。

12 ローカルサーバ機能を使用するパソコンの設定を行います。

[ローカルホスト]欄にローカルサーバ機能を使用するパソコンのIPアドレスを入力します。

13 [OK]ボタンをクリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示させてください。

14 [ローカルサーバ]の画面に戻ります。ローカルサーバで使用するサービスとパソコンのIPアドレスが表示されます。

15 [OK]ボタンをクリックします。

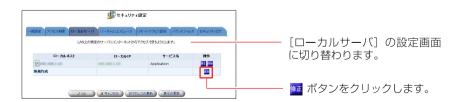
16 以上で設定は終了です。

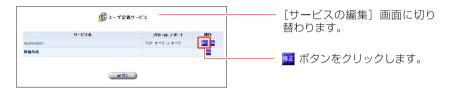
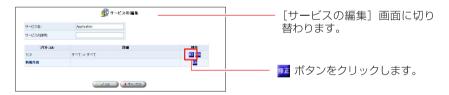
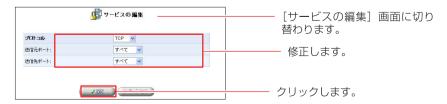
■ユーザ定義サービスの修正

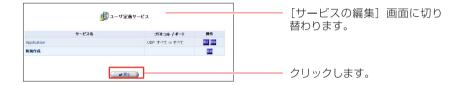
ここでは、既に作成したユーザ定義サービスを修正する方法について説明します。

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[ローカルサーバ]タブをクリックします。

3　設定を変更するパソコンの［修正］ボタンをクリックします。

4 [ローカルサーバの編集]画面が表示されます。
[ユーザー定義サービス]をクリックします。

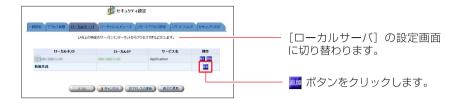
5 [ユーザ定義サービス]画面が表示されます。設定を変更したいサービスの［修正］ボタンをクリックします。

6 [サービスの編集]画面が表示されます。設定を変更したいプロトコルの［修正］ボタンをクリックします。

7 [サービスの編集]の画面が表示されます。設定を変更したい項目を修正し、[OK]ボタンをクリックします。

8　[OK]ボタンをクリックします。

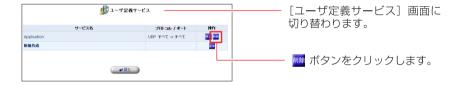
9　[ユーザ定義サービス]画面に戻ります。[戻る]ボタンをクリックします。

10　以上で設定は終了です。

■ユーザ定義サービスの削除

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[ローカルサーバ]タブをクリックします。

3 [新規作成]欄から［追加］ボタンをクリックします。

4 [ユーザ定義サービス]をクリックします。

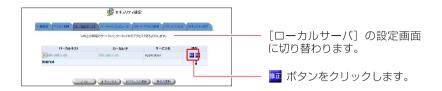
5 [ユーザ定義サービス]の画面が表示されます。削除したいサービスの［削除］ボタンをクリックします。

6 [戻る]ボタンをクリックします。

7 以上で設定は終了です。

設定したローカルサーバの修正

1 サイドバーから[セキュリティ設定]アイコンをクリックします。

2 [ローカルサーバ]タブをクリックします。

3　設定を変更したいパソコンの［修正］ボタンをクリックします。

4　［ローカルサーバーの編集］画面が表示されます。
使用するサービスまたはパソコンのIPアドレスを変更できます。

5　[OK]ボタンをクリックします。

6　以上で設定は終了です。

ローカルサーバの有効/無効の切替

1 サイドバーから[セキュリティ設定]アイコンをクリックします。

2 [ローカルサーバ]タブをクリックします。

3 [ローカルホスト]欄からサービスを無効にしたいIPアドレスのチェックを外します。

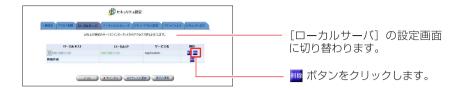
4 ［OK］ボタンをクリックします。

5 以上で設定は終了です。

設定したローカルサーバの削除

1 サイドバーから[セキュリティ設定]アイコンをクリックします。

2 [ローカルサーバ]タブをクリックします。

3　設定を削除したいサービスの［削除］ボタンをクリックします。

4　[OK]ボタンをクリックします。

5　以上で設定は終了です。

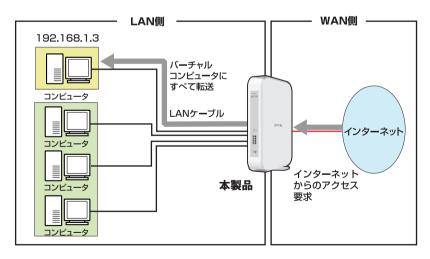
バーチャルコンピュータの設定

バーチャルコンピュータ機能を使用すると、LAN側にある1台のパソコンをインターネット上に公開できます。次のようなときに、バーチャルコンピュータを指定します。

・[ローカルサーバ]機能のリストにはないオンラインゲームやビデオ会議用のソフトウェアで、使用するポートなどの情報が公開されていない場合。

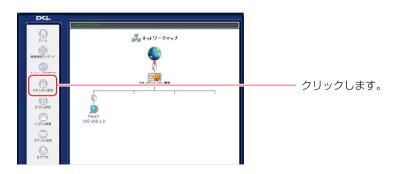
・セキュリティの制限無しに、1台のパソコンで全てのサービスをインターネットに公開する場合。

ご注意

・バーチャルコンピュータとして、複数のパソコンを設定することはできません。
・バーチャルコンピュータとして設定したパソコンは、ファイアウォールで保護されていないため、外部から攻撃を受ける恐れがあります。
・ローカルサーバ機能とバーチャルコンピュータ機能を同時に設定しているときは、ローカルサーバの設定が優先されます。
・DMZ（ポート）機能とバーチャルコンピュータ機能を同時に設定することはできません。

インターネットからLAN側へのアクセス要求を受け取ると、本製品は[ローカルサーバ]機能で登録されてる宛先を除き、すべてバーチャルコンピュータへその要求を転送します。

LAN側のパソコンをバーチャルコンピュータに設定する

■ バーチャルコンピュータ設定

1 サイドバーから[セキュリティ設定]アイコンをクリックします。

2 [バーチャルコンピュータ]タブをクリックします。

3 [バーチャルコンピュータ IPアドレス]欄にチェックを付け、バーチャルコンピュータにするパソコンのIPアドレスを入力します。

4 [OK]ボタンをクリックします。

5 以上で設定は終了です。

■ バーチャルコンピュータの有効/無効の切替

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[バーチャルコンピュータ]タブをクリックします。

3 [バーチャルコンピュータIPアドレス]欄からチェックを外します。

4 [OK]ボタンをクリックします。

5 以上で設定は終了です。

ダイナミックDNSの設定

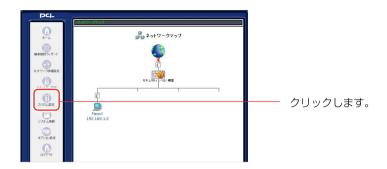
WEBサーバなどをインターネットに公開するときは、固定のグローバルIPアドレスが本製品に割り当てられている必要があります。しかし、インターネットに常時接続していても切断、再接続の際に動的にIPアドレスが変ってしまう場合があります。
ダイナミックDNSを使用すると、本製品のIPアドレスをダイナミックDNSサーバに一定間隔で通知することで、IPアドレスが変わった場合でも固定のホスト名が使用できます。
ダイナミックDNSは、下記に対応しています。
・DynDNS.org
・Dynamic DO!.jp
・MyDNS.JP

※「Dynamic DO!.jp」と「MyDNS.JP」は、「カスタム設定」から「ダイナミックDNS(国内のサービス)」を選択することで利用できます

! ご注意

・本製品は「www.dyndns.org」ダイナミックDNSサービスに対応しています。本製品のダイナミックDNSの設定を行う前に、「www.dyndns.org」にアクセスし、ユーザ名、パスワード、ホスト名の登録を行ってください。
・「www.dyndns.org」は、無償のサービスです(2005年9月現在)。
また、プロバイダによっては本設定を使わなくても、ダイナミックDNSを実現することが出来る場合があります。詳しくは、プロバイダにお問い合わせ下さい。

ダイナミックDNSの設定

1 サイドバーから[カスタム設定]アイコンをクリックします。
ここでは、DynDNS.orgを例に説明します。

2 [ダイナミックDNS(DynDNS.org)]アイコンをクリックします。

3 [ダイナミックDNS]の画面が表示されます。
[有効にする]欄にチェックを付け、ダイナミックDNSサービスに登録した内容をもとに各項目を入力します。

[ステータス]
現在の更新情報が表示されます。

[ユーザ名]
ダイナミックDNSサービスに登録されているユーザ名を入力します。

[パスワード]
ダイナミックDNSサービスに登録されているユーザパスワードを入力します。

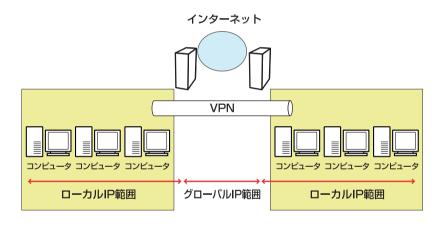
[ホスト名]
登録したホスト名とドメイン名を入力してください。

[メールサーバ]
メールサーバを登録したい場合は、メールサーバのホスト名を入力します。

4 [OK]ボタンをクリックします。

5 以上で設定は終了です。
設定が完了するとダイナミックDNSサーバへ本製品が取得しているIPアドレスを24時間毎に通知するようになります。

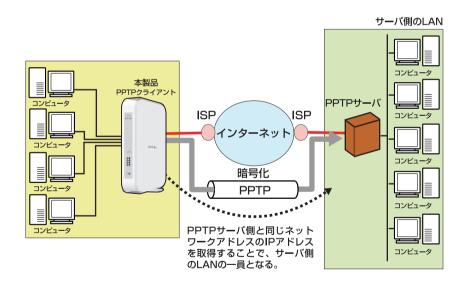
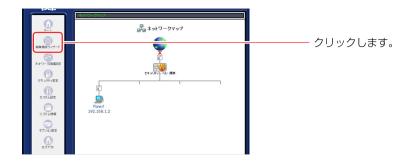
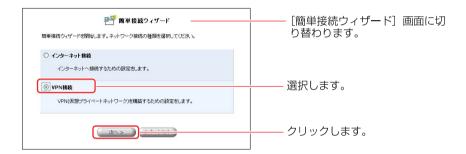
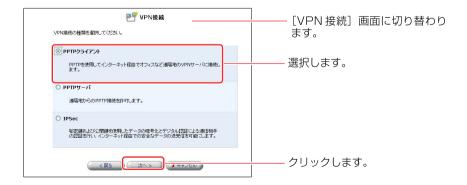
VPNの設定

VPN（Virtual Private Network）は、データのカプセル化や暗号化などのセキュリティ技術を使って、インターネットを仮想的に、専用線で接続したWANのように利用する技術です。VPNを構築するためには、PPTP（Point to Point Tunneling Protocol）やIPSec（IP Security）などのプロトコルが用いられます。
ここでは、PPTPとIPSecによるVPN接続の方法について説明します。
本製品は、PPTPサーバとPPTPクライアントおよびIPSecの機能を搭載しているため、パソコンにVPN用のソフトウェアを導入する必要もなく、強固なセキュリティ機能をもつVPNを構築することができます。

VPNを構築するには、簡単接続ウィザードによる設定をした後、ネットワーク詳細設定によって、詳細な設定が可能です。次ページの簡単接続ウィザードから設定を進めてください。必要に応じて、すでに簡単接続ウィザードによるVPN接続設定が終わっている場合は、「ネットワーク詳細設定による設定」に進んでください。

簡単接続ウィザードによる設定

ここでは、簡単接続ウィザードを使いVPNを構築する方法について説明します。本製品はPPTPサーバ、PPTPクライアント、IPSecに対応しています。ご利用する環境に合わせて設定を進めてください。
PPTPサーバと各クライアント、またはIPSecの各拠点は、LAN側をそれぞれ別のセグメントにする必要があります。

■PPTPクライアントの設定

本製品をPPTPクライアントとして使用する場合の設定について説明します。

1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。

2 [VPN接続]を選択し、[次へ]ボタンをクリックします。

3 [PPTP クライアント]を選択し、[次へ]ボタンをクリックします

4 リモートアクセスするサーバの設定に従い、PPTP接続の設定を行います。
[送信先のホスト名またはIPアドレス]に接続するPPTPサーバのIPアドレスを入力し、[接続ユーザ名]、[接続パスワード]に接続する時のユーザ名とパスワードを入力します。
[次へ]ボタンをクリックします。

PPTPクライアント

PPTP 接続の設定をします。

送信先のホスト名またはIPアドレス:

接続ユーザ名 (大文字/小文字に注意):

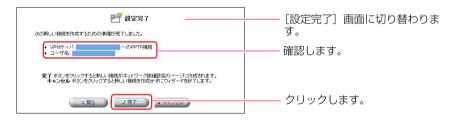
接続パスワード:

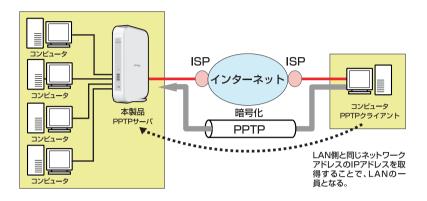
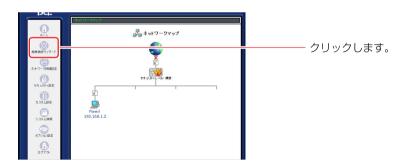
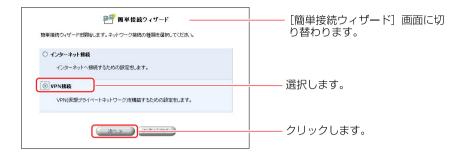
< 戻る　次へ >

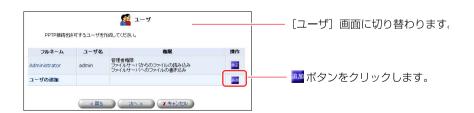
[PPTP クライアント] 画面に切り替わります。

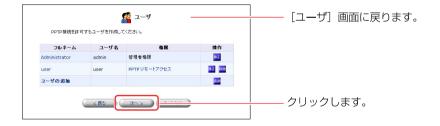
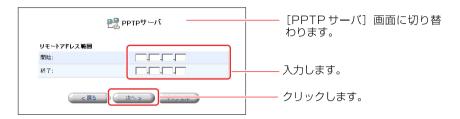
入力します。

クリックします。

5 [接続完了]画面が表示されます。
PPTP接続するサーバ名またはIPアドレスを確認し、[完了]ボタンをクリックします。

■ PPTPサーバの設定

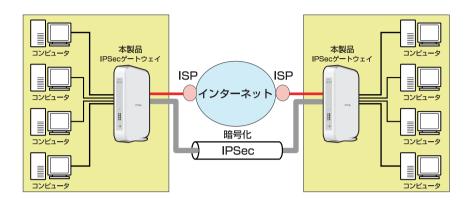
本製品をPPTPサーバとして使用する場合の設定について説明します。

1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。

2 [VPN接続]を選択し、[次へ]ボタンをクリックします。

3 [PPTP サーバ]を選択し、[次へ]ボタンをクリックします。

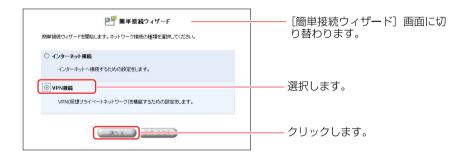
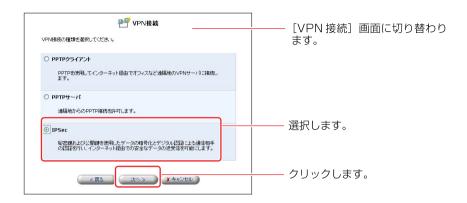
4 PPTP サーバにアクセスを許可する為のユーザ設定を行います。[ユーザの追加] の [追加] ボタンをクリックします。

5 [一般設定]欄のフルネーム、ユーザ名、新しいパスワード、新しいパスワードの確認に登録するユーザの設定を入力し、[権限]欄からPPTP リモートアクセスにチェックをつけます。

6 ユーザの追加または修正、削除が終わると[ユーザ]画面に戻りますので、[次へ]ボタンをクリックします。

7　**PPTPクライアントのリモートアドレスを入力します。**
PPTPサーバにリモートアクセスするユーザに割り当てるIPアドレスの範囲を入力し、[次へ]ボタンをクリックします。

8　**[設定完了]画面が表示されます。**
[完了]ボタンをクリックします。

インターネットに接続されている場合、PPTPクライアントの設定が完了すると、自動的にPPTPサーバへ接続を行います。

■ IPSecの設定

本製品を使いIPSecによるネットワーク同士のVPN接続を行う場合の設定について説明します。

1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。

2 [VPN接続]を選択し、[次へ]ボタンをクリックします。

3 [IPSec]を選択し、[次へ]ボタンをクリックします。

4 「ネットワークーネットワーク」を選び、[次へ]ボタンをクリックします。」

5 「リモートゲートウェイ」、「リモートサブネット」を選び、［次へ］をクリックします。

リモートゲートウェイ（イ）
指定したリモートゲートウェイアドレスからの接続だけを許可します。

すべてのリモートゲートウェイ（ロ）
すべてのリモートゲートウェイアドレスからの接続を許可します。

リモートサブネット（ハ）
指定したリモートサブネットからの接続を許可します。

すべてのリモートサブネット（ニ）
すべてのリモートサブネットからの接続を許可します。

6 接続するIPSecの情報を入力し、[次へ]ボタンをクリックします。
設定により入力する項目が異なる場合があります。

[接続先のホスト名またはIPアドレス]

IPSecで接続する相手側のIPアドレスを入力します。

[リモートサブネットアドレス]

IPsecで接続する相手側のネットワークアドレスを入力します。

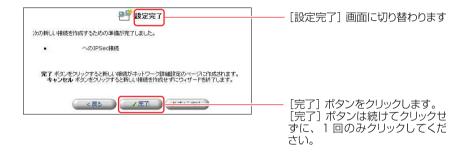
[リモートサブネットマスク]

IPSecで接続する相手側のサブネットマスクを入力します。

[シェアードキー]

IPSec間で認証を行うときに使う事前共有キーを入力します。

キーの値は両方のルータで同じ値を入力します。

7 [設定完了]画面が表示されます。[完了]ボタンをクリックします。

ワンポイント

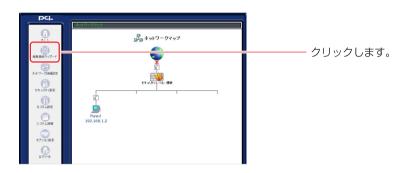
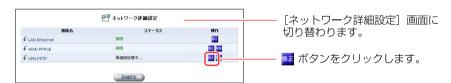
各ページの選択によって、設定する項目が異なります。

ネットワーク－ネットワーク	(イ) + (ハ)	ホスト名また IP アドレス
		リモートサブネット
		シェアードキー
	(イ) + (ニ)	ホスト名また IP アドレス
		シェアードキー
	(ロ) + (ハ)	リモートサブネット
		シェアードキー
	(ロ) + (ニ)	シェアードキー
ネットワーク－ホスト	(イ)	ホスト名または IP アドレス
		シェアードキー
	(ロ)	シェアードキー

ネットワーク詳細設定による設定

PPTPクライアントやサーバに関する詳細な設定と、IPSecの詳細設定について説明します。
VPNの詳細な設定をするためには、あらかじめ「簡単接続ウィザード」による設定を終了しておく必要があります。

■ PPTPクライアントの詳細設定

1 サイドバーから［ネットワーク詳細設定］アイコンをクリックします。

2 ［ネットワーク詳細設定］画面が表示されます。詳細な設定を行うVPN PPTP接続の［修正］ボタンをクリックします。

3 ［ネットワーク詳細設定 VPN PPTP］画面が表示されます。接続名、ステータス、ユーザ名等が表示されていますので、確認して［詳細設定］ボタンをクリックします。

4 ［詳細設定VPN PPTP］画面が表示されます。PPTPサーバ管理者の通知に従って設定します。

◎基本設定、PPP、PPP認証の設定

［PPP］

接続先のホスト名またはIPアドレス、接続ユーザ名、接続パスワードには、簡単接続ウィザードで設定した内容が表示されています。変更する必要がある項目を修正します。
自動切断までの時間は、PPTPによる通信が中断したときに接続を切断するまでの時間を分単位で入力します。

［PPP認証設定］

ユーザ認証のためのプロトコルを選択します。PPP暗号化で「暗号化を許可する」場合は、MS-CHAP またはMS-CHAP v2 を選択します。

◎PPP暗号化、IP設定

パケットの暗号化に関する設定を行います。

[PPP暗号化]

・暗号化を必ず要求する：
暗号化通信を要求するときにチェックします。サーバが拒否するとPPTP通信は確立されません。

・暗号化を許可する：
暗号化にMPPE（Microsoft Point-to-Point Encrypeion）を使用します。40bitのキーで暗号化するか、128bitのキーを使うかで、MPPE-40かMPPE-128を選択します。

・MPPE暗号化モード：
暗号化のモード（Stateless または Stateful）を選択します。Statelessはパケットごとに暗号化キーを変更するので、通信の安全性は高くなります。Statefulは複数のパケット単位で暗号化キーを変更します。
暗号化を許可する場合は、上のPPP認証で、MS-CHAPまたは、MS-CHAP v2が選択されていることを確認してください。

[IP設定]

IPアドレスを固定にするか、自動取得するかを選択します。
［サブネットマスクを置き換える］は、固定のサブネットマスクを利用するときにチェックし、そのときのサブネットマスクを指定します。

[DNSサーバ]

DNSサーバアドレスを自動取得するのか、固定設定にするのかを選択します。固定にする場合は、プライマリとセカンダリDNSサーバのIPアドレスを指定します。
なお、［DNSサーバ］をクリックすると、［カスタム設定］で［DNSサーバ］を選んだ状態になります。

[デバイスメトリック]

メトリックの値を入力します。

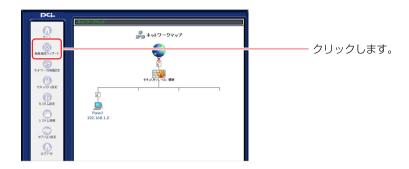
! ご注意

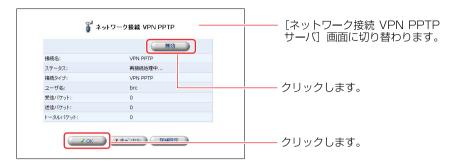
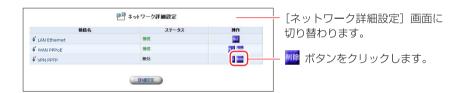
必ず［NAPT］は有効の状態でお使いください。

5 ［OK］ボタンをクリックすると設定が有効になり、［ネットワーク接続 VPN PPTP］画面に戻ります。

■PPTPクライアントの削除

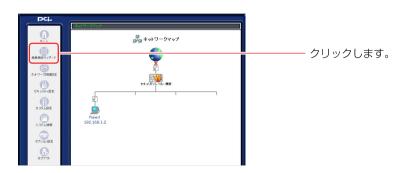
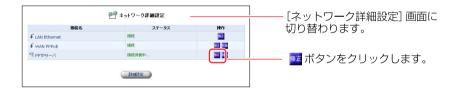
ここでは、既に登録してあるPPTPクライアント接続を削除する場合について説明します。

1　サイドバーから［ネットワーク詳細設定］アイコンをクリックします

2　[接続名]欄から削除するVPN PPTP接続の[修正]ボタンをクリックします。

3 回線が接続されてる場合は、[無効]ボタンをクリックし、回線をいったん切断します。[OK]ボタンをクリックします。

4 [接続名]欄から削除するVPN PPTP接続の[削除]ボタンをクリックします。

5 [戻る]ボタンをクリックします。

6 以上で設定は終了です。

■PPTPサーバの詳細設定

1 サイドバーから［ネットワーク詳細設定］アイコンをクリックします

2 ［ネットワーク詳細設定］画面が表示されます。詳細な設定を行うVPN PPTPサーバ接続の［修正］ボタンをクリックします。

※PPTPサーバを削除する場合は、［修正］ボタンをクリックし、［PPTPサーバ］画面の［有効］欄からチェックを外します。

3 ［PPTPサーバ］画面が表示されます。
［詳細設定］ボタンをクリックします。
なお、ここでユーザの編集、PPTPクライアントの接続設定も可能です。

4 ［PPTPサーバ］画面が表示されます。PPTPサーバの詳細な設定を行います。

［ステータス］

PPTPサーバの接続状況を表示します。

［有効］

PPTPサーバを有効にするときにチェックします。このチェックをはずすと、PPTPサーバとして動作しなくなり、接続状況にも反映されなくなり、また詳細設定の画面からも削除されます。

[自動切断までの時間]

PPTPによる通信が中断したときに、接続を切断するまでの時間を分単位で入力します。

[ユーザセキュリティ]

PPTPを使用した通信での認証と暗号化について設定します。

・認証が必要：
PPTPクライアントが接続するときに、ユーザ認証を必要とするときにチェックします。接続テストなど特別な場合を除いて必ずチェックを入れてください。

・暗号化が必要：
PPTPクライアントが接続するときに、暗号化通信を要求する場合にチェックします。

[許可する認証アルゴリズム]

ユーザセキュリティで認証が必要にチェックをした場合、認証のアルゴリズムをPAP、CHAP、MS-CHAP-v1、MS-CHAP-v2　から選択します。暗号化をする場合は、 MS-CHAP-v1かMS-CHAP-v2をチェックしてください

[許可する暗号化アルゴリズム]

ユーザセキュリティで暗号化が必要にチェックをした場合、暗号化アルゴリズムをMPPE-40 と MPPE-128 から選択します。

[MPPE暗号化モード]

暗号化のモード（Stateless または Stateful）を選択します。

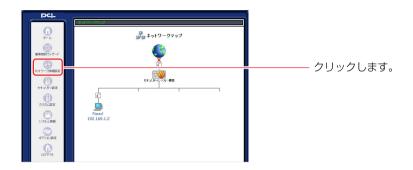
・Stateless ：
パケットごとに暗号化キーを変更するので、通信の安全性は高くなります。

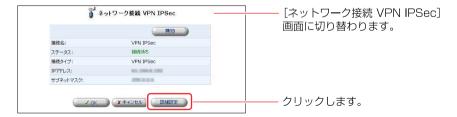
・Stateful ：
複数のパケット単位で暗号化キーを変更します。

5 ［簡単接続ウィザード］で設定した、リモートアドレス、クライアントとして動作する場合のPPTPクライアントの設定が表示されます。クリックし修正することが可能です。

6 ［OK］ボタンをクリックすると、設定が有効になりネットワーク詳細設定画面に戻ります。［基本設定］ボタンをクリックすると、PPTPサーバの最初の画面に戻ります。

■IPSecの詳細設定

1　サイドバーから［ネットワーク詳細設定］アイコンをクリックします

2　［ネットワーク詳細設定］画面が表示されます。詳細な設定を行うVPN IPSec接続の［修正］ボタンをクリックします。

3　［ネットワーク接続 VPN IPSec］画面が表示されます。［詳細設定］ボタンをクリックします。

4 「詳細設定 VPN IPSec」画面が表示されます。

ここで次の項目を設定します。

基本設定

[接続先のホスト名またはIPアドレス]

簡単接続ウィザードで設定した接続先が表示されています。必要であれば修正します。

[ローカルサブネット]

本製品のLAN側のサブネットアドレス、サブネットマスクを設定します。

[リモートサブネット]

接続先のサブネットアドレスとサブネットマスクを入力します。

[データ圧縮]

データ圧縮をするときにチェックします。

[キー交換方式]

暗号化アルゴリズムや鍵交換のためのSAの合意をとる方式を選択します。

・自動：
IKE（Internet Key Exchange）を使って、SAの合意を通信時に自動的に行う場合に選択します。通常は、自動に設定しておきます。

・手動：
SAの合意をあらかじめ手動で設定しておく場合に選択します。画面が手動用に切り替わります。

! ご注意

必ず手動モードは「トンネリング」の状態でお使いください。

5 キー交換方式を自動に設定します。

キー交換方式を［自動］に設定した場合、次の2つのフェーズの設定を行います。まず、IPSec IKE, Phase 1の設定をします。

IPSec IKE, Phase 1

［接続試行回数］

ネゴシエーションの試行回数を設定します。

［ライフタイム］

キーの有効期限を秒単位で設定します。

［Rekey Margin］

Rekey（キーの再生成）を期限切れの何秒前に開始するかを設定します。

［Rekey Fuzz］

Rekey Marginをランダムに変更するパーセンテージを設定します。

［認証アルゴリズム］

認証の方式を選択します。

・シェアードキー方式：
共通キー方式を選択する場合は、事前共有キーの文字列を入力します。
（かんたん設定ウィザードで入力した鍵が表示されます。）

・公開キー方式：
公開キー方式を使用する場合に、キーの文字列を入力します。

［暗号化アルゴリズム］

使用する暗号化アルゴリズムをチェックします。

［ハッシュアルゴリズム］

使用するハッシュのアルゴリズムをチェックします。

［Diffie-Hellman-Group］

対応するグループをチェックします。

6 次にIPSec IKE, Phase 2の設定をします。

IPSec IKE, Phase 2

[ライフタイム]

キーの有効期限を秒単位で設定します。

[PFS有効]

Secrecy(PFS)を使用する場合にチェックします。

[AH]

認証ヘッダの設定をします。ハッシュアルゴリズムを選択します。

[ESP]

暗号ペイロードの設定をします。暗号化アルゴリズムと認証アルゴリズムの設定をします。

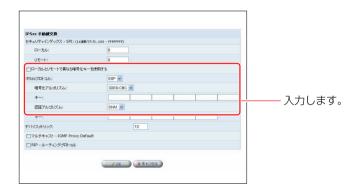
[デバイスメトリック]

メトリックの値を入力します。

7 [詳細設定 VPN IPSec]画面の設定内容を確認し、［OK］ボタンをクリックして、設定を有効にします。

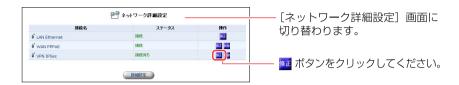
8 IPSecを利用しVPNを構築する場合は、IPフラグメントパケットを透過させる必要がありますので、［セキュリティ設定］画面で、［IPフラグメントパケットを遮断する］のチェックをはずしてください。

■キー交換方式を手動に設定する場合

キー交換方式で手動を選択したときは、接続先の設定にあわせて暗号化アルゴリズム、認証アルゴリズムを設定する必要があります。

暗号化アルゴリズム、認証アルゴリズムのキーは、16進数8桁ずつに区切って入力してください。

■ VPNの接続、切断

サーバ側、クライアント側でインターネットに接続すると、自動的にLAN同士が接続されます。

1 IPSecによる通信を切断したい場合は、［ネットワーク詳細設定］画面で、［VPN IPSec］の［修正］ボタンをクリックします。

2 ［ネットワーク接続VPN IPSec］画面になりますので、［無効］ボタンをクリックします。

IPSec接続に関してその他次の設定が可能です。

■キーの再生成

1　サイドバーから［カスタム設定］アイコンを選択します。

2　［IPSec］アイコンをクリックします。

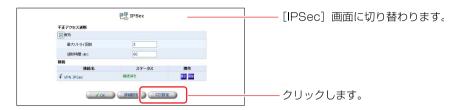
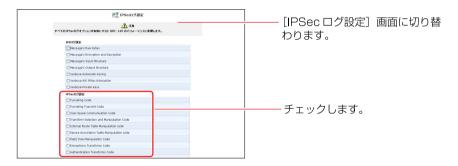
3　［IPSec］画面が表示されます。［詳細設定］ボタンをクリックします。

4 [IPSec設定]画面が表示されます。[キーの再生成] ボタンをクリックし、再生成を行います。

5 表示の更新ボタンをクリックすると、再生成されたキーが表示されます。[戻る] ボタンをクリックすると [IPSec] 画面に戻ります。

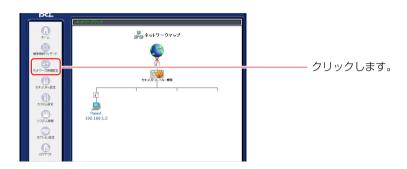
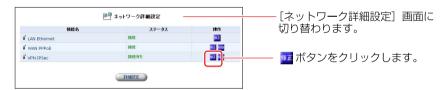
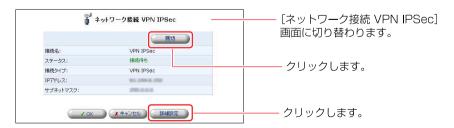
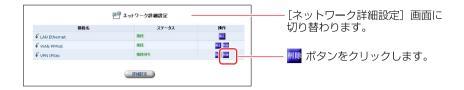
■IPSecログの設定

IPSec通信のログに関する設定を変更することができます。

1 カスタム設定で[IPSec]アイコンをクリックし、IPSec画面で[ログ設定]ボタンをクリックします。

2 [IPSecログ設定]画面が表示されます。記録したい内容にチェックをつけます。

3 [OK]ボタンをクリックすると設定が有効になり、[IPSec]画面に戻ります。

IPSecの削除

ここでは、既に登録してあるIPSec接続を削除する場合について説明します。

1　サイドバーから［ネットワーク詳細設定］アイコンをクリックします

2　[接続名]欄から削除するVPN IPSec接続の[修正]ボタンをクリックします。

3　回線が接続されてる場合は、[無効]ボタンをクリックし、回線をいったん切断します。[OK]ボタンをクリックします。

4 [接続名]欄から削除するVPN IPSec接続の[削除]ボタンをクリックします。

5 以上で設定は終了です。

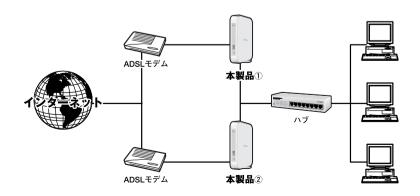
オプション設定

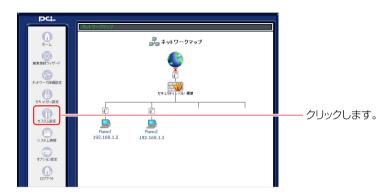
ここでは、本製品を利用してオプション機能を設定します。本製品の設定は、有線LAN接続でおこなってください。

VRRP

本製品は、VRRP機能に対応しており、ルータの冗長化を行うことができます。
VRRPを設定することで、通常利用している回線・ルータが何らかの理由により切断されたときに、同一グループ内のルータが自動的に通信が継承できます。
この機能を使用するためには、VRRP機能に対応した複数のルータを1つのグループに所属させておく必要があります。
以下の設定例を使用して紹介します。

[設定例]
各ルータに実際に存在しない仮想IPアドレスを設定し、マスタールータからの回線が何らかの原因で不具合が発生したとき、バックアップルータが代わりに通信を開始します。

	マスタールータ（本製品①）	バックアップルータ（本製品②）
IPアドレス	192.168.50.250	192.168.50.250
VRRP ID	1	1
優先度	250	100
プリエンプトモード	有効	有効

1 設定例イメージのように接続し、マスタールータ側にログインします。

2 サイドバーから［カスタム設定］アイコンをクリックします。

3 「カスタム設定」が表示されますので、[VRRP]アイコンをクリックします。

4 「VRRP」が表示されますので、「仮想ルータの追加」をクリックします。

5 「VRRP設定」が表示されますので、下記項目を設定します。
①「IPアドレス」に「192.168.50.250」を入力します。
②「VRRP ID（1-255）」に「1」を入力します。
③「優先度」に「250」を入力します。
④「プリエンプトモードを有効にする」のチェックをオンにします。
⑤「監視対象」で監視する対象を選びます。
⑥ [有効]ボタンをクリックします。

6 続いて、バックアップルータ側の設定を行います。バックアップルータにログインし、2から5の手順をおこないます。

7 「VRRP設定」が表示されますので、下記項目を設定します。
①「IPアドレス」に「192.168.50.250」を入力します。
②「VRRP ID（1-255）」に「1」を入力します。
③「優先度」に「100」を入力します。
④「プリエンプトモードを有効にする」のチェックをオンにします。
⑤「監視対象」で監視する対象を選びます。
⑥ [有効]ボタンをクリックします。

以上で、設定が完了しました。

! ご注意

[本製品]

・DHCPサーバ機能は、[無効]に設定することをお勧めします。

[各コンピュータ側]

①IPアドレスを手動で設定し、「デフォルトゲートウェイ」に仮想IPアドレスを設定します。設定例の場合は、「192.168.50.250」です。
②DNSサーバは、プロバイダから指定されたDNSサーバを設定することをお勧めします。

［IPアドレス］

VRRPで利用する仮想ルータのIPアドレスを設定します。クライアントのデフォルトゲートウェイアドレスにはこのIPアドレスを設定します。

○同じVRRP IDに属するルータのIPアドレスを指定するとき
仮想ルータのIPアドレスを持つルータがマスタルータとなり、他のルータはバックアップルータになります。

○実在しないIPアドレスを指定するとき
マスタルータは優先度の設定によって自動的に決定されます。IPアドレスは同一サブネットのIPアドレスを設定します。

［VRRP ID］

仮想ルータで利用するグループのIDを設定します。値は1～255までの数値で設定します。初期値は0です。
VRRP IDを同じ値に設定したルータは同一グループに属し、1台がマスタルータとして動作し他はバックアップルータとして動作します。
マスタルータ停止時に、バックアップルータへ処理を移行し、通信を継続します。

［VRRP送信間隔］

VRRPに設定されたルータがLANへ送信するパケットの送信間隔を設定します。単位は秒です。初期値は1秒です。
マスタルータがパケットを送信し、バックアップルータが受信することでVRRPが動作していることがわかるようになります。

［優先度］

VRRPで動作するルータの優先度を設定します。値は1～255までの数値で設定します。初期値は100です。値が大きいほど優先度は高くなります。

［プリエンプトモードを有効にする］

プリエンプトモードを設定します。プリエンプトモードの設定でマスタルータの選ばれ方が変わります。

○プリエンプトモードが有効のとき
VRRPで動作するルータに優先度の高いルータが加わるとマスタルータが移行します。有効で利用されることをお勧めします。

○プリエンプトモードが無効のとき
マスタルータ停止時などでバックアップルータへ移行したあと、優先度の高いVRRPのルータが加わってもマスタルータは移行しません。

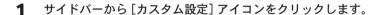
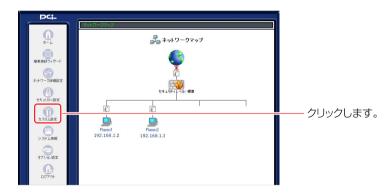
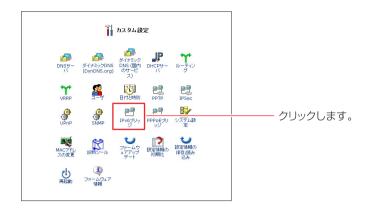
［監視対象］

既存の接続から監視対象を選びます。

IPv6ブリッジ

本製品は、IPv6ブリッジ機能に対応しています。WAN-LAN間の通信データをブリッジすることができます。
これにより、通常のPPPoEによるインターネット接続とFLET'S.NETなどのIPv6ネットワークをLAN側に設置されたパソコンで同時にご利用頂くことが可能になります。

※パソコンのIPv6設定については、お使いのパソコン及びOSの取扱説明書などを参照してください。

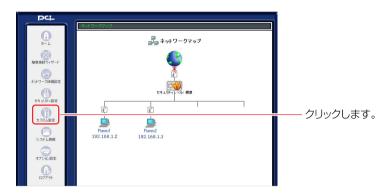
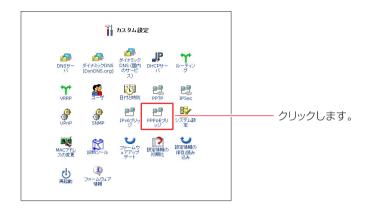
1 サイドバーから［カスタム設定］アイコンをクリックします。

2　［IPv6ブリッジ］アイコンをクリックします。

3　「IPv6ブリッジを有効にする」のチェックをオンにします。

4　［OK］ボタンをクリックします。

PPPoEブリッジ

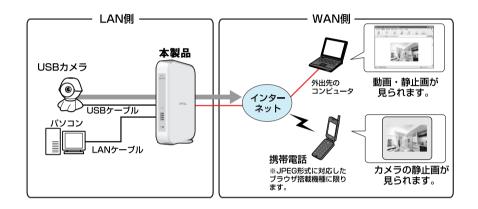
本製品は、PPPoEブリッジ機能に対応しています。本機能を利用することで、LAN側に接続したパソコンが直接PPPoE接続して通信することができます。

※パソコンのPPPoE接続の設定については、お使いのパソコン及びお使いの取扱説明書をご覧ください。

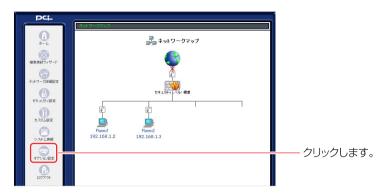
1 サイドバーから［カスタム設定］アイコンをクリックします。

2　「PPPoEブリッジ」をクリックします。

3　「PPPoEブリッジを有効にする」のチェックをオンにします。

4　[OK] ボタンをクリックします。

USBカメラの設定

本製品のUSBインタフェースに接続したUSBカメラ（別売）で撮影した静止画や動画を、リモートアクセスしたPCや携帯電話で見ることができます。
ここでは、USBカメラを有効にする設定と画像を見る方法について説明します。
本体に接続できるUSBカメラは1台のみです。

※本機能は、USBカメラ「BRC-EE260」にのみ対応しています。その他のUSBカメラには対応していません。本製品へのUSBカメラ接続方法は、USBカメラ「BRC-EE260」の取扱説明書をご参考ください。

USBカメラ設定

1 サイドバーから［オプション設定］アイコンをクリックします。

2 ［オプション設定］画面が表示されます。[USBカメラ]アイコンをクリックします。

3 ［USBカメラ］設定画面が表示されます。本製品にUSBカメラ接続後、「オン」にチェックをつけます。

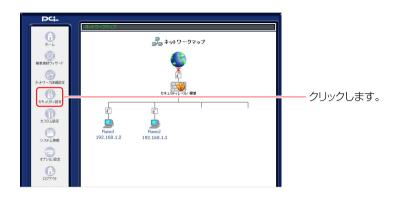
ご注意

・［USBカメラ］設定画面の「オン／オフ」は、デフォルトの設定が「オフ」になっています。
・USBカメラが「オン」の状態でカメラを取り外すと、自動的に「オフ」に切り替わります。

4 ［画像ビットレート］から［高（512Kbps）］または［低（128Kbps）］のいずれかを選択します。

5 ［OK］ボタンをクリックします。
USBカメラの撮影とストリーミングの画像の配信が自動的に始まります。

■インターネットからカメラ画像を見る場合

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［セキュリティ設定］画面が表示されます。［リモートアクセス］ボタンをクリックします。

3 ［リモートアクセス設定］画面が表示されます。
［WEBサーバを外部に公開する（プライマリポート）］または［WEBサーバを外部に公開する（セカンダリポート）］から使用していないポート番号の方にチェックし、［USBカメラ画像を外部に公開する（TCPポート8090）］にチェックをつけます。

4 ［OK］ボタンをクリックします。

5 以上で設定は終了です。

■画像を見るための条件

USBカメラで取り込んだ画像をPCや携帯電話で見る場合、コンピュータや携帯電話の種類によって以下のソフトウェアや条件が必要となります。

端末	静止画サイズ	動画サイズ	必要なソフトウェア・条件
Windows®	320×240	320×240	Microsoft®Internet Explorer5.5以上 Netscape Navigator®6.0以上 Microsoft®Windows®Media Player7.0以上
Macintosh®	320×240	320×240	Microsoft®Internet Explorer5.5以上 Netscape Navigator®6.0以上 Microsoft®Windows®Media Player Mac板 (Windows®Media Player for Mac OS®X, Windows®Media Player 7.1 for Mac OS®8-9
Linux	320×240	320×240	Netscape Navigator®6.0以上 Mplayerなど
携帯電話	112×96	なし	JPEG画像をサポートしている機種のみ。 機種によっては利用できない場合があります。

■コンピュータで画像を見る

本製品にパソコンからリモートアクセスして、画像を見る方法について説明します。

1 ブラウザから、URLを指定してリモートアクセスします。

・インターネットからアクセスする場合
「http://(WAN側アドレス)/cam/」

・LANからアクセスする場合
「http://(LAN側アドレス)/cam/」

2 本製品にリモートアクセスすると、ログイン認証を行ないます。すでに登録してあるユーザ名とパスワードを入力してください。はじめてアクセスするときは、事前にログインユーザ名、パスワードを設定しなければなりません。設定方法は、180ページの「ログインユーザ名とログインパスワードの設定」を参照してください。

※なお、この認証機能は、撮影された画像・動画を特定の相手にのみ公開することを完全に保証するものでありません。

3 ログイン認証終了後、[BRC-14VG・ライブカメラ](BRC-W14VGのときは[BRC-W14VG・ライブカメラ])画面が表示されます。画面にあるメニューから、観覧するカメラ画像の種類を選択します。

[カメラ画像・静止画]
クリックすると静止画のページを表示します。

[カメラ画像・動画]
クリックすると動画のページを表示します。

[カメラページトップ]
このメインページを表示します。

メニュー項目を選択することで、どの画面からでも随時切り替えることできます。

4 ［カメラ画像・静止画］を選択した場合、「ライブカメラ静止画像」画面が表示されます。［更新］ボタンをクリックすると、現在の画像を更新します。

5 ［カメラ画像・動画］を選択した場合、「ライブカメラ動画」画面が表示されます。

ご注意

・動画配信の場合、ネットワークの状況やWindows® Media Playerのバッファリング処理等のため、画像が表示されるまでに時間がかかる場合があります。
・動画、静止画ともに画像の輝度、コントラストなどの調整を行うことはできません。

■携帯電話で画像を見る

本製品に携帯電話からリモートアクセスして、画像を見る方法について説明します。

1 携帯電話のブラウザから、URLを指定してリモートアクセスします。

・携帯電話用アドレス：http://（WAN側アドレス）/i/

2 本製品にリモートアクセスすると、ログイン認証を行ないます。すでに登録してあるユーザ名とパスワードを入力してください。はじめてアクセスするときは、事前にログインユーザ名、パスワードを設定しなければなりません。設定方法は、180ページの「ログインユーザ名とログインパスワードの設定」を参照してください。

3 ログイン認証終了後、画像表示用のメインページが表示されます。［更新］ボタンをクリックすると、現在の画像を更新します。

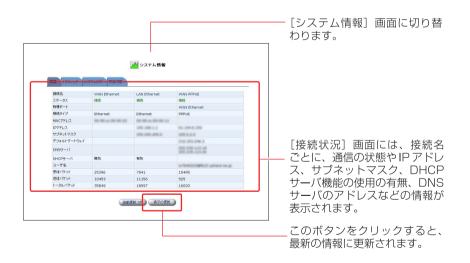
保守・管理

本製品の運用開始後にネットワークの接続状態の確認や、管理者のログイン名やパスワードの変更方法などを説明します。本製品の設定は、有線LAN接続でおこなってください。

機器状況の確認

接続状態の確認

各接続ポートごとに通信状態やアドレス情報等が確認できます。

1 サイドバーから［システム情報］アイコンをクリックします。

［WAN Ehternet］

PPPoE以外の方法でインターネットに接続している場合の、WAN側の通信の状況が確認できます。

［WAN PPPoE］

PPPoEでインターネットに接続している場合のWAN側の通信の状況が確認できます。

［LAN Ehternet］

LAN側の通信の状況が確認できます。

［VPN PPTP］

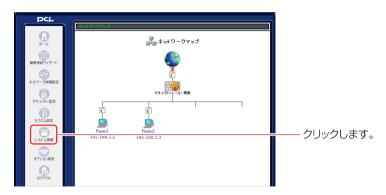
本製品がPPTPクライアントである場合の通信の状況が確認できます。

［VPN IPSec］

IPSecで通信している状況が確認できます。

稼動時間の確認

ここでは本製品が稼動してからの現在までの時間を確認できます。

1 サイドバーから［システム情報］アイコンをクリックします。

2 ［稼動時間］タブをクリックします。

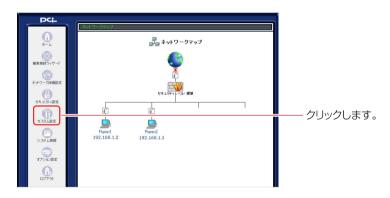
●画面表示の自動更新を停止する
［カスタム設定］画面－［システム設定］画面で［システム情報ページの表示の自動更新を行う］をチェックしているときは、［システム情報］の各画面は一定間隔で自動更新されます。このとき、［システム情報］の各画面の［自動更新Off］ボタンをクリックすると、［表示の更新］ボタンをクリックした時のみ、［システム情報］の各画面の内容が更新されるようになります。

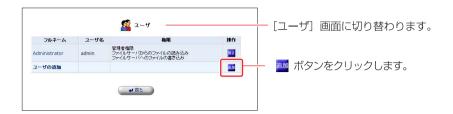
ログインユーザ名・ログインパスワード設定

本製品のログインユーザ名とパスワードの登録、変更、または削除ができます。
ユーザは50以内とすることをお勧めします。
※50以上のユーザを設定すると、本製品の動作パフォーマンスに影響することがあります。

ログインユーザ名とログインパスワードの設定

■ユーザの新規作成

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［ユーザ］アイコンをクリックします。

3 ［ユーザの追加］欄から「追加」ボタンをクリックします。

4 ［ユーザ設定］画面が表示されます。
フルネーム、ユーザ名、新しいパスワードを入力します。

［フルネーム］

登録するユーザのフルネームを入力します。半角英数字で128桁まで入力できます。

［ユーザ名］

新しく登録するユーザのログイン名を入力します。半角英数字で64桁まで入力できます。

［新しいパスワード］

ユーザがログイン時に使用するパスワードを入力します。半角英数字で64桁まで入力できます。
大文字と小文字は区別されますのでご注意ください。

［新しいパスワードの確認］

「新しいパスワード」と同じパスワードを再度入力します。

5 本製品での権限を設定します。

［管理者権限］

ユーザを管理者として登録する場合は、チェックします。

［PPTP リモートアクセス］

PPTP によるVPN接続を許可する場合は、チェックします。

［ファイルサーバからのファイルの読み込み］

USBハードディスク接続時に、ディスク内のファイルの読み込みを許可する場合は、チェックします。

［ファイルサーバからのファイルの書き込み］

USBハードディスク接続時に、ディスク内のファイルの書き込みを許可する場合は、チェックします。

［USBカメラ］

USBカメラ接続機能に、カメラ画像の閲覧を許可する場合は、チェックします。

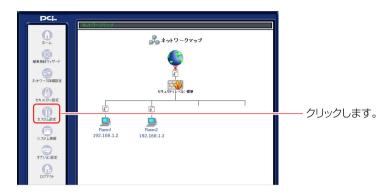
6 E-mail通知を利用する場合は、E-mailアドレス、システム通知レベル、セキュリティ通知レベルを設定します。

※E-mail通知機能に関してはE-mail通知機能をご参照ください

7 ［OK］ボタンをクリックします。

8 以上で設定は終了です。

■ユーザの修正

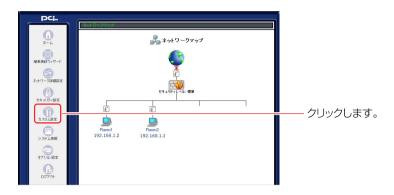
1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［ユーザ］アイコンをクリックします。

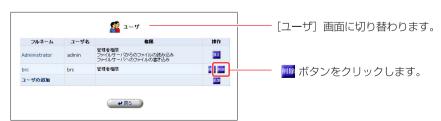
3 設定を変更したいユーザの［修正］ボタンをクリックします。

4 ［ユーザ設定］画面が表示されます。修正したい項目の変更を行い、［OK］ボタンをクリックします。

5 以上で設定は終了です。

■ユーザの削除

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［ユーザ］アイコンをクリックします。

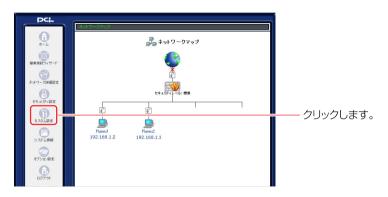
3 設定を削除したいユーザの「削除」ボタンをクリックします。

! ご注意

購入時に登録されてるAdministratorは削除することができません。

4 以上で設定は終了です。

システム設定

本製品のホスト名やLAN側のドメイン名などを設定できます。

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［システム設定］アイコンをクリックします。

3 ［システム］欄に本製品のホスト名、ドメイン名を入力します。

［ホスト名］

本製品のホスト名を入力します。

［ローカルドメイン］

LAN内で使用したいドメイン名を入力します。

4 USBハードディスクを接続している場合、［ファイルサーバ］欄から［NetBIOSワークグループ名］を入力します。

［NetBIOSワークグループ名］

LAN内で使用するワークグループ名を入力します。

5 ［設定画面］欄から［システム情報ページの表示の自動更新を行う］、［ネットワーク設定の変更時に確認を行う］を設定します。

［システム情報ページの表示の自動更新を行う］

［システム情報］画面の表示を自動的に更新させたい場合は、チェックします。

［ネットワーク設定の変更時に確認を行う］

ネットワークに関する変更をしたときに、確認メッセージを表示させたい場合は、チェックします。

6 ［システムリモートログ設定］、［セキュリティリモートログ設定］を利用する場合は設定をします。

※リモートログ設定に関しては、Syslogの設定をご参照ください。

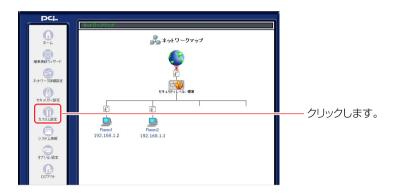
7 ユーザ設定でE-mail通知機能を利用している場合は、［SMTPメールサーバ］欄にメールサーバのアドレスを入力します。

8 ［OK］ボタンをクリックします。

9 以上で設定は終了です。

日付と時刻の設定

本製品の日付や時刻の設定を変更できます。

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［日付と時刻］アイコンをクリックします。

3 手動設定する場合は、新しい日付と時刻を入力します。

4 自動設定する場合は、［自動設定］欄から［有効］にチェックします。

5 ［NTPサーバアドレス］、［更新間隔］を入力します。

［NTPサーバアドレス］

指定したアドレスから時刻を指定します。

［更新間隔］

時刻を更新する間隔を指定します。

6 ［OK］ボタンをクリックします。

7 以上で設定は終了です。

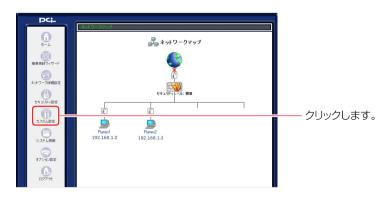
ファームウェアの更新

本製品の購入後、当社のホームページからダウンロードしたファイルを使って、最新のファームウェアにアップデートすることができます。ファームウエアのアップデートの前には、本製品の設定内容を書き残し、必ず有線LAN接続するコンピュータでおこなってください。

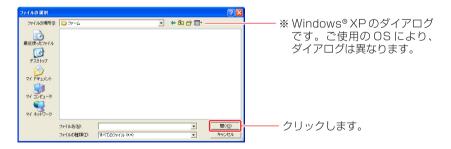
！ご注意

・インターネットに接続している場合は、アップデートを行う前に全ての通信を切断してください。また、LAN内のパソコンはアップデート作業を行うパソコンを除いて全て電源をOFFにしてください。
・ファイアウォールやウィルススキャンソフトがインストールされてるパソコンでアップデート作業を行う場合は、事前にソフトウェアを終了してください。
・このアップデートは当社が独自に提供するサービスです。新機能の追加や性能の増強を保証するものではありません。
・ファームウエアの更新中は、他の操作をおこなったり、本製品のACアダプタ、LANケーブルは絶対に抜かないでください。ファームウエアの更新の失敗や、本製品の故障の原因となる場合があります。

1 当社のホームページから最新のファームウェアをダウンロードします。
ダウンロードしたファイルは、アップデート作業を行うパソコンのハードディスクなどに保存してください。

2 サイドバーから［カスタム設定］アイコンをクリックします。

3　［ファームウェアアップデート］アイコンをクリックします。

4　［ファームウェアアップデートの準備］の画面が表示されます。
［参照］ボタンをクリックし、ダウンロードしたファームウェアのファイルを指定します。

5　［開く］ボタンをクリックします。

6 ［OK］ボタンをクリックすると、ファームウェアアップデートの準備が開始されます。

! ご注意

ファームウェアアップデートの準備中は、絶対に本製品の電源を切ったり、LANケーブルを抜いたりしないでください。ファームウェアアップデートの準備には、数十秒間かかります。［OK］ボタンをクリックしたら、そのまましばらくお待ちください。

7 ファームウェアアップデートの準備が終了すると、［ファームウェアアップデート］の画面が表示されます。
［現在のバージョン］と［新しいバージョン］に表示されるバージョン番号に間違いが無いか確認してください。
［OK］ボタンをクリックすると、ファームウェアのアップデートが開始されます。

! ご注意

ファームウェアのアップデート中は、絶対に本製品の電源を切ったり、LANケーブルを抜いたりしないでください。ファームウェアアップデートには、数十秒間かかります。［OK］ボタンをクリックしたら、そのまましばらくお待ちください。

8 アップデートが終了すると、本製品は自動的に再起動します。新しいバージョンのファームウェアは再起動後に有効になります。

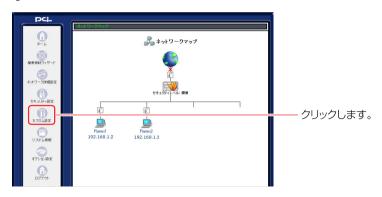
9 再起動が完了すると、ログイン画面に戻ります。以上でファームウェアの更新は終了です。

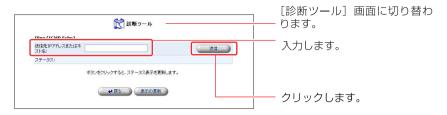
! ご注意

本製品以外のファームウェアを使ってアップデートを行うことはできません。無理にアップデートを行うと本製品が動作しなくなりますので、ご注意ください。

診断ツール

本製品からパソコンなどのネットワーク端末に対してPingを送信することができます。

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［診断ツール］アイコンをクリックします。

3 ［送信先IPアドレスまたはホスト名］欄にPingを送信したいIPアドレスまたはホスト名を入力します。

4 ［送信］ボタンをクリックすると、本製品から宛先にPingが送信されます。

5 ［ステータス］欄に送信結果が表示されます。

6 ［戻る］ボタンをクリックします。

7 以上で設定は終了です。

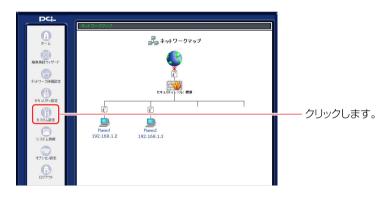
本製品の初期化

設定ページから本製品の設定内容を消去して、購入時の状態に戻すことができます。

※本体にあるリセットスイッチを使って、設定を消去することもできます。

ご注意

この機能を使うと、設定ページにアクセスするためのパスワードを含め、変更した設定内容がすべて消去されます。また、本製品のLAN側ポートのIPアドレスを変更していた場合は、購入時の「192.168.1.1」に戻ります。ご注意ください。

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［設定情報の初期化］アイコンをクリックします。

3 ［OK］ボタンをクリックします。

4 初期化が始まります。

5 設定内容の消去が終わると、設定ページに初めてログインするときの画面に切り替わります。

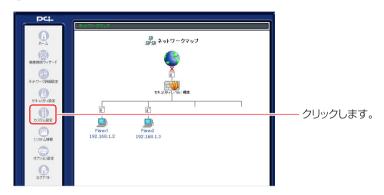
※画面が切り替わらないときは、［ログイン］ボタンをクリックしてください。

6 ユーザ名とパスワードを入力し、[OK] ボタンをクリックします。
[ネットワークマップ設定画面] に切り替わります。

[ログインユーザ名]	設定ページにログインするユーザ名を入力します。
[新しいログインパスワード]	パスワードを入力します。
[新しいログインパスワードの確認]	[新しいログインパスワード] の内容をもう一度入力します。

7 [OK] ボタンをクリックすると、設定ページの [ネットワークマップ設定画面] に切り替わります。

設定情報の読み込み

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 カスタム設定の［設定情報の保存/読み込み］アイコンをクリックします。

3　［設定情報の読み込み］ボタンをクリックします。

4　［設定情報の読み込み］の画面が表示されます。
［参照］ボタンをクリックし、設定ファイルを指定します。

5　［開く］ボタンをクリックします。

6　［OK］ボタンをクリックすると、設定情報の読み込みの準備が開始されます。

7 設定情報の読み込みの準備が終了すると、［設定情報のアップデート］の画面が表示されます。

［現在のバージョン］と［新しいバージョン］にはファームウェアのバージョンが表示されます。
バージョンが同じことをご確認の上、［OK］ボタンをクリックしてください。

ご注意

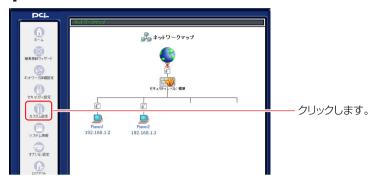
・［現在のバージョン］と［新しいバージョン］にはファームウェアのバージョンが表示されます。

・ファームウェアのバージョンが異なると設定情報のアップデートができない場合がありますのでご注意ください。

8 アップデートが終了すると、本製品は自動的に再起動します。新しい設定情報は再起動後に有効になります。

9 再起動が完了すると、ログイン画面に戻ります。以上で設定情報の読み込みは終了です。

設定情報の保存

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　カスタム設定の［設定情報の保存/読み込み］アイコンをクリックします。

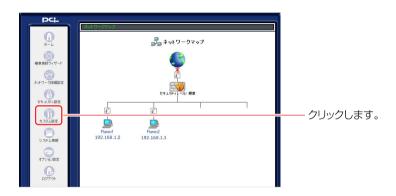
3　［設定情報の読み込み］ボタンをクリックします。

4　［ファイルのダウンロード］の画面が表示されます。［保存］ボタンをクリックしてコンピュータに保存します。

5　以上で設定情報の保存は終了です。

再起動

本製品の再起動を行います。

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［再起動］アイコンをクリックします。

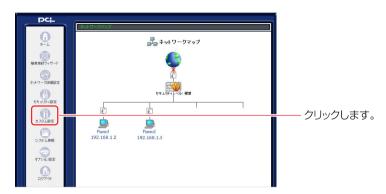
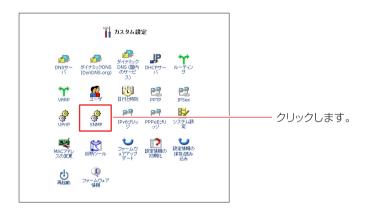
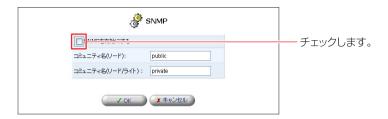
3 ［OK］ボタンをクリックします。

4 再起動が完了すると、ログイン画面に切り替わります。

SNMP

SNMPを設定することで、ネットワークに接続された機器類をネットワーク経由で監視することができます。

※SNMP機能を使用するためには、別途SNMPマネージャなどが必要です。

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［SNMP］アイコンをクリックします。

3 「SNMPを有効にする」のチェックをオンにし、コミュニティ名（セキュリティ）を入力します。

［コミュニティ名（リード）］

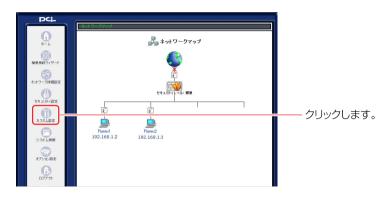
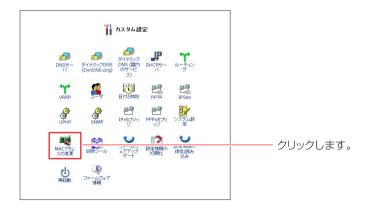
監視対象サーバのステータスを収集するのみのセキュリティ（コミュニティ）を設定します。初期値は、「public」になります。

［コミュニティ名（リード/ライト）］

サーバの設定変更（ディスクスレッショルドの設定や、IMLの消去等）に伴う操作を行うときのセキュリティ（コミュニティ）を設定します。初期値は、「private」となります。

MACアドレスの変更

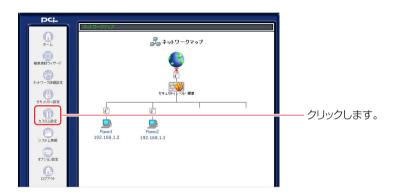
MACアドレスで接続を管理しているときなど、機材を変更することによって接続ができなくなる場合があります。そのようなことを避けるためにも、MACアドレスを手動で変更することができます。

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 「MACアドレスの変更」アイコンをクリックします。

3 変更したいMACアドレスを入力します。

4 ［OK］ボタンをクリックします。

ファームウェア情報

本製品のファームウェアのバージョンを確認できます。

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［ファームウェア情報］アイコンをクリックします。

3 本製品のファームウェアのバージョンが表示されます。